AL/CF-TR-1996-0159

UNITED STATES AIR FORCE
ARMSTRONG LABORATORY

COGNITIVE ENGINEERING FOR INFORMATION DOMINANCE: A HUMAN FACTORS PERSPECTIVE

Randall D. Whitaker

LOGICON TECHNICAL SERVICES, INC.
P.O. BOX 317258
DAYTON, OH 45437-7258

Gilbert G. Kuperman

CREW SYSTEMS DIRECTORATE
HUMAN ENGINEERING DIVISION
WRIGHT-PATTERSON AFB, OH 45433-7022

OCTOBER 1996

INTERIM REPORT FOR THE PERIOD JULY 1995 TO OCTOBER 1996

19970410 096

Approved for public release; distribution is unlimited

Crew Systems Directorate
Human Engineering Division
2255 H Street
Wright-Patterson AFB, OH 45433-7022

DTIC QUALITY INSPECTED 3

NOTICES

When US Government drawings, specifications, or other data are used for any purpose other than a definitely related Government procurement operation, the Government thereby incurs no responsibility nor any obligation whatsoever, and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data, is not to be regarded by implication or otherwise, as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use, or sell any patented invention that may in any way be related thereto.

Please do not request copies of this report from the Armstrong Laboratory. Additional copies may be purchased from:

National Technical Information Service
5285 Port Royal Road
Springfield, Virginia 22161

Federal Government agencies and their contractors registered with the Defense Technical Information Center should direct requests for copies of this report to:

Defense Technical Information Center
8725 John J. Kingman Road, Suite 0944
Ft. Belvoir, Virginia 22060-6218

TECHNICAL REVIEW AND APPROVAL

AL/CF-TR-1996-0159

This report has been reviewed by the Office of Public Affairs (PA) and is releasable to the National Technical Information Service (NTIS). At NTIS, it will be available to the general public, including foreign nations.

This technical report has been reviewed and is approved for publication.

FOR THE COMMANDER

Kenneth R. Boff

KENNETH R. BOFF, Chief
Human Engineering Division
Armstrong Laboratory

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
October 1996

3. REPORT TYPE AND DATES COVERED
Interim, July 1995 to October 1996

4. TITLE AND SUBTITLE
Cognitive Engineering for Information Dominance: A Human Factors Perspective

5. FUNDING NUMBERS
C: F41624-94-D-6000
PE: 62202F
PR: 7184
TA: 10
WU: 46

6. AUTHOR(S)
*Randall D. Whitaker
Gilbert G. Kuperman

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
*Logicon Technical Services Inc.
P.O. Box 317258
Dayton, OH 45437-7258

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Armstrong Laboratory, Crew Systems Directorate
Human Engineering Division
Human Systems Center
Air Force Materiel Command
Wright-Patterson AFB OH 45433-7022

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AL/CF-TR-1996-0159

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

Information Warfare (IW) is emerging as the critical military issue of the day. IW is introduced and analyzed with respect to its major themes and current definitions. Those aspects of IW requiring cognitive engineering research are identified, necessary methodological reorientations are outlined, and key links to the human factors/cognitive engineering topics of situation awareness and decision making are discussed. A specific target capability (the common battlespace picture) and the framework for research toward that goal (the OODA model) are introduced. The OODA model is contextualized with respect to other relevant research areas and U.S. Air Force practices. An integrated cognitive engineering program for IW analyses is specified and illustrated with respect to an example drawn from theater missile defense (TMD) attack operations. Extensive listings of bibliographic references, terminological definitions, and relevant Internet resources provide a solid foundation for further reading and research.

14. SUBJECT TERMS
information warfare, information dominance, dominant battlespace awareness, cognitive engineering, OODA loop, situation awareness, decision making.

15. NUMBER OF PAGES
127

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Standard Form 298 (Rev. 2-89) (EG)
Prescribed by ANSI Std. 239.18
Designed using Perform Pro, WHS/DIOR, Oct 94

This page intentionally left blank.

PREFACE

This technical report summarizes work toward formulating a coherent vision of the emergent area of *information warfare (IW)* and those aspects of IW which are amenable to human factors research. The diverse definitions of IW share one common theme -- that information and the systems through which information is processed are increasingly critical components in modern warfare. As 'centers of gravity,' information systems and their contents have become key assets exploitable for offensive advantage and deserving of defensive protection. This document therefore concentrates on those human factors issues pertaining to individual and collective information processing within theater military operations -- a scope matching that area of research termed *cognitive engineering*.

The first goal of this report was to delineate a coherent IW vision. This was accomplished via a comprehensive review of the burgeoning IW literature and a conceptual analysis of the field's scope and essential dimensions. The second goal of the report was to specify the direction and nature of constructive cognitive engineering research supporting American IW efforts. This required that we establish an approach to IW which links the informational aspects of modern warfighting (e.g., intelligence gathering, data fusion, communications) with the instrumental actions (e.g., attacks, sorties) by which modern war is prosecuted. We have done this by adopting and elaborating upon a specific model for tactical battle analysis (Colonel John Boyd's *OODA Loop* construct). The final goal of this report was to define an integrated cognitive engineering approach which would provide the methodological framework for analyzing actual operations with respect to IW issues. We have accomplished this by first outlining an integrated program incorporating data collection, analysis, and application tactics, then illustrating the course of this program with a concrete example drawn from theater missile defense attack operations.

The work summarized herein was conducted during the period 1 July 1995 through 30 September 1996 within the USAF's Crew-Aiding and Information Warfare Analysis Laboratory (CIWAL) -- a component of the Fitts Human Engineering Division of Armstrong Laboratory. The project manager was Gilbert Kuperman of AL/CFHI. The work was conducted under support contract F41624-94-D-6000 by Logicon Technical Services, Inc. (LTSI), PO Box 317258, Dayton OH 45437-7258.

The authors wish to gratefully acknowledge the substantial contributions of two CIWAL colleagues. Mr. Robert E. Smith (Senior Systems Analyst, LTSI) generated and compiled the EADSIM simulation data used in the missile defense example. The efforts of Ms. Elisabeth Fitzhugh (Senior Human Factors Technician, LTSI) greatly facilitated the massive literature search upon which this document was based.

This page intentionally left blank.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

I. INTRODUCTION

It has become both fashionable and illuminating to analyze military history in terms of its evolution with respect to warfighting technologies. The most detailed of these analyses (e.g., Ellis, 1975, on the machine gun) have focused on specific weapons, the course of their adoption, and the results of their introduction. Such fine-grained studies have the advantage of addressing artifacts in the narrow context of purely military utility. This keeps the discussion relatively free of ambiguities and confusions regarding reciprocal or parallel events outside the scope of the military enterprise.

On a broader scale, there have been analyses claiming that more general technical innovations in the society at large have resulted in significant -- even "revolutionary" -- transformations in warfighting both as a specific activity and as a component of the socio-political enterprise. This type of historical transformation is currently labeled a *military technical revolution (MTR)*. The label, attributed to Soviet military theorists in the late 1970's, denotes the phenomenon where "...extreme transformations in warfare occurred as a result of the exploitation of technology." to achieve "...operational and organizational innovations" (Lee, 1994, p. 3, credited to Krepinevich, 1992, p. 3). The technical innovations motivating these broader military transformations range from chariots to nuclear weapons (cf. Keegan, 1993). Listings and classifications of the resulting "military revolutions" vary with particular authors' specific mappings of technology to warfighting, their chronologies, the granularity of their categories, and the like. A representative illustration is provided by Krepinevich (1994), who outlines ten such "military revolutions" occurring from the fourteenth century forward:

- The *Infantry Revolution* in which foot soldiers achieved a dominant role (over cavalry)
- The *Artillery Revolution*
- The *Revolution of Sail and Shot*, in which naval vessels transformed into sail-powered gunnery platforms
- The *Fortress Revolution*, in which fortifications adapted to artillery appeared
- The *Gunpowder Revolution*, in which firearms for foot soldiers evolved
- The *Napoleonic Revolution* in logistics and organization
- The *Land Warfare Revolution* in firepower, transportation, and communication
- The *Naval Revolution* of steam, iron, and submarine

• The *Nuclear Revolution*

It is overly simplistic to attribute determinative causal power to technological innovation per se. Technical innovation is only the seed of the process through which warfighting is revolutionized -- it changes the affordances or means through which combatants may pursue their ends. Technology cannot revolutionize any enterprise (military or not) until it is recognized, developed, and adopted. To give but one example, the employment of artillery (ca. the 14th century) occurred long after gunpowder's invention (ca. 950 A.D.) and far from its point of origin (China). The role of technology in war has, however, become so much a cliché that military planners no longer await -- but actively pursue -- innovation of means. In the twentieth century, the clear (but not decisive) relationship between technical mastery and military superiority has made technical innovation a focus of military planning and spending. It is this proactive approach to technological issues which motivates work such as this study.

There is wide agreement that the form of warfighting is currently undergoing significant transformations constituting an MTR (cf. Fitzsimonds, 1995; Krepinevich, 1994). This most recent transformation is typically analyzed with respect to the proliferation of advanced *information technology (IT)* in military operations. The label most commonly applied to this current MTR is the *Revolution in Military Affairs (RMA)*. The terms "MTR" and "RMA" are sometimes used to denote both a generic technical-military transformation and the currently perceived transformation (Krepinevich, 1992; Mazarr, 1994). For the sake of clarity, we shall reserve the term "MTR" for the generic case and employ "RMA" to denote the present IT-driven change(s) of compelling interest to the American defense community.

Exploitation of IT is taken to be the means for the emergent transformation in warfighting. This focus on IT is well-evidenced by the Information Technology and Information Applications Volumes in the landmark study *New World Vistas* (U.S. Air Force Scientific Advisory Board, 1995). To the extent that IT is assumed to be the key to future warfare innovations, the diverse analyses of the RMA concur. However, all consensus disappears when the subject turns to the operational ends to be served by this IT exploitation -- i.e., the specific types of military activities to be revolutionized through IT. These break down into two general categories:

• Those concerned with exploiting IT to enable one's own military system to operate more efficiently and more effectively than it did before. Own-system features are the targets for change, and the criteria for improvement are based

on own-system performance.

- Those concerned with exploiting IT to enable one's own military system to obtain advantageous leverage over an adversary's military system. The balance of own-system features vs. relevant adversary-system features is the target for change, and the criteria for improvement are based on relative own-system vs. adversary-system performance. This may encompass actively degrading the adversary's IT capabilities.

Success in one can facilitate success in the other, but there is no necessity that they entail each other. As a result, projects to accomplish the one do not necessarily entail accomplishing the other. The confusion deriving from these conflicting foci has been exacerbated by their all being lumped together under the rubric of *information warfare (IW)*.

Both the above-listed categories of IT exploitation target performance in warfighting. In both cases, performance is treated as a function of capacities for communicating and processing information -- e.g., acquiring data, fusing them into an input stream, correlating this input stream with current knowledge, projecting outcomes, weighing alternatives, deciding a course of action, enacting the decision, and coordinating the process of enactment. As a result, progress in both categories of IW innovations will be driven by research into, and development of, optimum communications and information processing on the part of warfighters.

Such work falls squarely into the category of *cognitive engineering* -- the application of analytical and engineering principles to issues of human cognitive performance as a means to improve cognition-relevant features of practical tools and methods. This label was coined by Donald Norman (1981), whose explanations of the necessity for and scope of a cognitive engineering endeavor are discussed in later works (Norman, 1984; Norman, 1986; Norman, 1987). Cognitive engineering derives from the theoretical area of *cognitive science*, which spans "...psychology, artificial intelligence, linguistics, sociology, anthropology, and philosophy." (Norman, 1987, pp. 325-326) Norman considers this range of sources necessary because "(t)he combination seems essential, for each of the disciplines contributes an essential point of view and body of techniques, theories, and knowledge that is missed by the others." (*Ibid.*) Moving from the realm of pure science to that of applied science, Norman concludes that "...(i)f the combination of the sciences yields cognitive science, then perhaps the combination of the applied areas of the disciplines should yield a cognitive engineering." (*Ibid.*)

Cognitive engineering, then, is the application of relevant parts of the pure cognitive sciences to the design and construction of information systems that engender effective interaction between the artifacts and the people they support. Rasmussen (1986) explains cognitive engineering's payoffs by stating that "(q)ualitative models identifying categories of behavior and the limiting properties of the related human resources will serve designers well in the design of systems that allow humans to optimize their behavior within a proper category." (pp. 61-62) This payoff is to be obtained through the introduction of end user models as foundational elements in the total system design. Although Rasmussen's more recent work has employed the term *cognitive systems engineering* to denote this area (Rasmussen, Pejtersen and Goodstein, 1994), we shall use the original term in this document.

This study will therefore proceed from a cognitive engineering perspective -- one which focuses upon the informational aspects of performance in military operations. These informational aspects are relevant to the extent they result in effective instrumental action -- i.e., to the extent they result in decisive action. The critical juncture of informational and instrumental performance is *decision* -- the process through which knowledge guides action. Our perspective will therefore center on the decision makers comprising a given military system.

To the extent that technologies span both military and non-military applications, the clarity and focus of weapons-specific analyses cannot be achieved. The RMA's technological base (IT) pervades modern life and defies simplistic analysis as a purely military phenomenon. In addition, we face the problem of focusing on this phenomenon from within its flow, as it is occurring. In response to both these complicating factors, we must labor to construct and maintain an orderly account of this necessarily confusing area.

It is no overstatement to claim that the flurry of discussion on IW or "fog of war" theory has engendered an unfortunate "fog of war theory." A tangle of jargon -- some redundant, some contradictory -- has arisen around the whole subject. As a result, we must attempt to untangle and straighten out the lexicon before we can constructively proceed. In the course of this document we shall explore numerous definitions and connotations, attempt to sort them out, and delineate their importance. To anchor our discussion, we shall specify wherever possible the terms of choice and our manner of employing them. The reader is cautioned to pay attention to our lexical specifications, which are not universally reflected in the IW literature. To aid the reader, and to provide a long-term reference source, a glossary of IW terminology is provided along with an extensive bibliography.

II. THE CURRENT RMA

The RMA is treated as an evolutionary advance or paradigm shift, with IT as its catalyst. Given current widespread discussion of IT's current and future effects, the "Information Revolution" will be taken as given, and no background review will be undertaken here. The point is that the proliferation of IT has had "revolutionary" effects, and the RMA represents recognition of the military ramifications. Insufficient attention to the ramifications of some earlier military technologies has demonstrably led to disaster. This danger is well illustrated by Ellis' (1975) analysis of how European blindness and intransigence in adopting and deploying machine guns contributed to unnecessary carnage in WWI trench warfare. The intense interest in the current RMA is intended to avoid the same sort of mistake.

Visions of the RMA share widespread allusions to three sources of thematic inspiration -- the projections of futurists Alvin and Heidi Toffler (1980; 1990; and especially their 1993 book *War and Anti-War*), the ancient Chinese classic *The Art of War* by Sun Tzu, and the extraordinary success of operations Desert Shield / Desert Storm during the Persian Gulf War. We shall briefly review these three thematic exemplars in an attempt to sort out their relevance in understanding the RMA. The review will illustrate why IW is promoted as the harbinger of tomorrow's strategies, the final operationalization of long-standing wisdom, and the current best explanation for recent military success. Finally, we shall briefly note two other areas (*semiotics* and *post-modern textuality*) of active scholarly interest which have not yet been recognized for their relevance to understanding the RMA and information warfare.

II.A. The Tofflers: The Third Wave and its Associated War Form

During the last three decades, Alvin and Heidi Toffler have authored several popular accounts of societal transformation (1970; 1980; 1990). Because they analyze history via simple schemata drawn with broad strokes, their work is better described as journalism from a broad perspective rather than detailed socio-historical scholarship. Nonetheless, the accessibility of the Tofflers' books has resulted in their being widely read, which in turn has made them perhaps the most common point of reference in analytical future studies outside academe. Of primary relevance to the current RMA / MTR debate is the Tofflers' categorization of civilizations to

date into three major "waves" (1: agrarian; 2: industrial; 3: informational), distinguished by the emergence and evolution of a particular economic form (1980; 1990). Their most recent thesis is that each wave has in turn generated one or more corresponding "war forms" in which military ends and means have evolved in conformance with the dominant economic form (Toffler & Toffler, 1991).

The Tofflers claim we are in the midst of a transition between the second and third waves. According to them, the last three centuries have marked the period of *second-wave* economies and associated war forms. This second wave began in the wake of the Renaissance, swelled through the Enlightenment and reached its concrete fruition with the Industrial Revolution. Although the Industrial Revolution is usually ascribed to the late 18th and early 19th centuries, the Tofflers date the beginning of the second wave to the late 17th century (cf. Toffler & Toffler, 1991, p. 18). The seminal event was the rise of Newtonian science and the subsequent proliferation of several key ideas: "...the idea of progress; the odd doctrine of individual rights; the Rousseauian notion of a social contract; secularism; the separation of church and state; and the novel idea that leaders should be chosen by popular will, not divine right." (Toffler & Toffler, 1991, p. 20) Second-wave warfare has emphasized warfighters drawn from a general pool of citizens, a professional officer class, authority concentrated in hierarchies, forces gauged by their mass (e.g., manpower, firepower), and strategies geared to mass action in pursuit of focused decisive outcomes. Clausewitz is the canonical theorist of second-wave warfare, and World Wars I and II are canonical examples of second-wave war.

In the Tofflers' vision of the emerging *third-wave* economy, the dominant productive work form is "knowledge work," usually in support of service provision. Such activity is aimed at ever more finely delineated niches, conducted by constantly-shifting alliances among players, and supported by increasingly sophisticated information networks (Toffler & Toffler, 1990). The existence of a flexible and ubiquitous medium for communication and commerce (e.g., the "Net") is presumed to necessarily facilitate activities which: (a) reflect the medium's flexibility in terms of scale, connectivity, duration, aims, and processes and (b) reflect the medium's ubiquity in terms of accessibility, scope, and functionalities. Prospective third-wave economies and war forms are predicted to entail unending novelties and complexities in the number and character of players, distributed authority, forces gauged by their precise effects, and strategies geared to fine-

grained actions in pursuit of general outcomes contributing to ongoing developments.

Generally, the notion of transformations in work corresponding to the rise of information technologies has been a long-standing theme. As the visions of Vannevar Bush (1945) and Douglas Engelbart (1988a; 1988b) evolved into the marketable commodity of the Internet, analyses and projections of impacts have broadened from the workplace to society at large. Such enquiry is now just as fashionable in the military (e.g., Sullivan and Dubik, 1994). The Tofflers (1991; 1993) imply it was their vision that inspired the last decade's reconsideration of American military doctrine in the light of the "information revolution." Regardless of their true impact, it must be acknowledged that their work has provided the most public entry point to the ideas now associated with the RMA / MTR.

This is not to say that the Tofflers' historical analysis and vision is perfect, being as it is a simplified account tailored for popular consumption. DiNardo and Hughes (1995) criticize the Tofflerian allusions in RMA / IW discussions, deriding without elaboration the Tofflers' approach as simplistic and rife with errors of detail. Their critique is constructive to the extent it highlights the fact that relevant historical transformations are considerably more complex than the Tofflers' simple "1-2-3" formulation. This is of crucial importance to professional historians (such as DiNardo and Hughes), but such quibbles do not invalidate the utility of the Tofflers' analysis for its intended "popular" (i.e., non-academic) audience -- of which military professionals are members.

Perhaps more relevant is that Dinardo and Hughes' challenge to the Tofflers has no apparent bearing on the current issue of concern -- the IT-driven RMA. The focus of their criticism is the transition from "first wave" to "second wave," which they understandably but erroneously address exclusively in terms of the Industrial Revolution from ca. 1800 onward (cf. the explanation of "second wave" above). Because they do not address the transition of immediate interest -- "second wave" to "third wave" -- their critique of the Tofflers is essentially tangential to RMA / IW considerations.

II.B. Sun Tzu: The Acme of Skill and Means Other than War

Sun Tzu's *The Art of War* (1963) has become a canonical reference point in IW literature. It is a (probably fragmentary) compendium of military theory largely unknown in the West until the 20th century. The work derives from the period known as that of the "Warring States," running from ca. 453 to ca. 300 B.C. (cf. Griffith, 1963, pp. 20-29). This era of constant war among China's factious kingdoms constituted:

> "...one of the most chaotic periods in China's long history. The forested hills, the reed-bordered lakes, the many swamps and marshes provided hiding places for the bands of robbers and cut-throats who raided villages, kidnapped travellers, and exacted toll from merchants unlucky enough to fall into their hands. Many of these outlaws were peasants who had been forced into brigandage to survive. Others were escaped criminals, deserters from the army, and disgraced officials. Altogether they constituted a formidable challenge to the so-called forces of law and order." (*op cit*, p. 21)

During the period of the Warring States, Chinese princes schemed to further purposes that "...could be served in the China of that time only by intrigue or war" (*op cit*, p. 25), between which no firm distinction was made. The time was ripe for what we now call consultants:

> "...hundreds of scholars who wandered from one state to another ... eager to peddle ideas to rulers 'anxious over the perilous condition of their countries and the weakness of their armies'. Sovereigns competed for the advice of battalions of professional talkers, who in 'interminable discussions', captivated kings, dukes, and great men with arguments of 'confusing diversity'." (*op cit*, p. 24)

Sun Tzu's success was in being the first such scholar of warfare to provide the requisite "...coherent strategic and tactical theory and a practical doctrine governing intelligence, planning, command, operational, and administrative procedures." (*op cit*, p. 25) DiNardo and Hughes (1995) question the importance of Sun Tzu in IW circles, trivially challenging *The Art of War* on the basis of its Chinese cultural context; its age; its brevity (e.g., compared with Clausewitz); and its "aphoristic style" (p. 3). Moreover, they find it odd that a "first-wave thinker" should be so

inspirational for "third-wave" theorists. This last point, at least, is a substantive topic for discussion.

Sun Tzu's popularity is in large part a reaction to all things second-wave, from which we are clearly diverging. The dominant military theorist of the second wave was Clausewitz, whose philosophy of war and dogmatic resistance to recognizing modes of warfare other than his "native" Napoleonic style has been the subject of recent scholarly criticism (e.g., Keegan, 1993). The critique typically proceeds as follows. Clausewitz treated war as the open, total, and unrestricted prosecution of political initiatives by lethal means. In his wake, military science pursued efficient and effective means for such purposes, with science advancing the state of the art and second-wave industry advancing the state of the armory. These advances in means outstripped progress regarding ends or understanding of war's relation to other societal activities. Second-wave warmaking therefore increasingly took on the one-dimensional character of a technological contest. The two World Wars and the Cold War illustrate the results.

In the simultaneous presence of obvious change and absence of new theory, one often looks to the most (apparently) relevant available candidate(s). Within the context of military science, and in the face of the perceived RMA, Sun Tzu is seen to provide the most (apparently) available relevant alternative to Clausewitz. This is based on contrasts between Sun Tzu and Clausewitz (cf. Handel, 1991). DiNardo and Hughes (1995) miss the point in focusing on ancient Chinese "first-wave" agrarianism, textual brevity, and aphoristic generalities. *The Art of War* is popular because it is seen to resonate (at least in part) with the current situation. This in turn is due to contextual similarities between the period of the Warring States and our current post-Cold War world.

Just as "war and intrigue" were interwoven in the period of the Warring States, recent militarism seems less akin to formal second-wave war and more like a general *warfare* -- "...the set of all lethal and non-lethal activities undertaken to subdue the hostile will of an adversary or enemy." (Szafranski, 1995, p. 57). Warmaking is increasingly interlinked with economic, social, cultural, and similar "systems other than the political." As a result, success in accomplishing political goals is not comprehensively correlated with success in second-wave warfighting. Proliferating "low intensity conflicts" are certainly not characterizable as Napoleonic / Clausewitzian contests between matched opponents on open ground. For this

reason alone, Sun Tzu is worthy of renewed interest because of his influence on guerrilla / insurgency warfare by way of Mao Tse-Tung (cf. Griffith, 1963, pp. 45-56).

In Sun Tzu's China, there was relative technological parity among competitors -- standing armies, brigands, and insurgents. Combatants typically were drawn from within China, affording an additional measure of parity in terms of culture, language, and value systems. This comprised a relatively finite, steady-state playing field. Successful warfighting under these conditions had to prioritize informational tactics and tactical information as tools of leverage where instrumental means were not predictably decisive. In Sun Tzu's steady-state agrarian world, advantage was obtained by being deceptive in form, fluid of act, and capable of countering skilled responses in kind. Such finesse was not so critical in Clausewitz's expansionist industrial world, where advantage (most often technical) allowed combatants to be explicit in form, ponderous of act, and attuned to responses in kind.

The expansionism of the last few centuries is bringing us around to a relatively finite playing field. Technological disparities are being reduced through the self-limitations of weapons of most massive destruction and the increased availability of more modest arms. Most relevant to IW is the increased accessibility to IT and through this to the worldwide data / communication networks. Although major disparities still exist among culture, language, and belief systems, the global trend toward connectivity is inducing a measure of homogeneity. The world is not yet as homogeneous as Sun Tzu's ancient China, but it is certainly becoming more so each year. If Vietnam was the "living room war" of the 1960's in the United States, Desert Storm was the "living room war" of the 1990's for the world at large.

Just as in China during the period of the Warring States, the political map is being continuously redrawn. Today's global political stage is clearly something other than the second wave's clear-cut landscape of nation states (cf. the significance of the United Nations, Amnesty International, Greenpeace, the Palestine Liberation Organization, etc.). Increasingly, one must wonder if a viable map is possible. The networks enacting militaristic action (e.g., terrorist groups) and invoking militaristic intervention (e.g., drug cartels) have become as ephemeral and "transnational" as large corporations. The localized open ground of Clausewitz's battlefields has given way to the global shadow battlespaces of urban undergrounds, "back channels," and satellite news feeds. In this shadow landscape, territory is marked by informational

concord rather than geographic extent.

Whatever the "third wave" proves to be, its nascent complexities bear somewhat more resemblance to Sun Tzu's world than to Clausewitz's. However, it is important to note that today's emergent scenario is not isomorphic with Sun Tzu's China. The relative technological and social parities are the result of complexity rather than uniformity. The trend of territorialization (literal and figurative) is toward diversification rather than consolidation. The relevance of Sun Tzu to the RMA is best summarized as this: then, as now, the remaining opportunities for advantageous leverage entail informational (or at least information-intensive instrumental) means. This is the most defensible basis for embracing *The Art of War* as a metaphorical guide to currently emergent war forms. Beyond this, Sun Tzu is an opportunistic reference recommended mainly by its availability in the face of change. (Interestingly, Keegan (1993) characterizes the renewed interest in Clausewitz following World War II as a similarly opportunistic development in response to demands for a policy suited to the new technology of nuclear weapons.)

This notion of exercising finesse within constraints of finitude explains why IW literature is full of allusions to Sun Tzu's notion of the "acme of skill" -- the ability to subdue an enemy without recourse to direct confrontation in open combat. *The Art of War* illustrates this concept with many anecdotes in which communication between adversaries induced perception of implications (of either relative commonality or inequality) motivating a resolution with little or no bloodshed. Owing to the pervasive references to this "acme of skill," we should examine the full passage in which it is elucidated -- the opening of Sun Tzu's chapter on "Offensive Strategy":

> " 1. Generally in war the best policy is to take a state intact; to ruin it is inferior to this.
>
> 2. To capture the enemy's army is better than to destroy it ...
>
> 3. For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill.
>
> 4. Thus, what is of supreme importance in war is to attack the enemy's strategy.
>
> 5. Next best is to disrupt his alliances.
>
> 6. The next best is to attack his army.
>
> 7. The worst policy is to attack cities."

(Sun Tzu, 1963, pp. 77-78)

Success in surpassing and suppressing an adversary's capacities can be achieved partially or wholly by the adept manipulation of information, knowledge, and beliefs. To the extent that an adversary's view of a situation can be manipulated, one might degrade or even nullify that enemy's military aims, his will to pursue them, and his means for prosecuting them. This is what Sun Tzu means when he claims "All warfare is based on deception." (1963, p. 66) Moreover, this provides the direct link to the idea that future warfare will be informational in nature. Success in a contest of reciprocal deception boils down to a matter of knowledge creation and exploitation, best illustrated in the closing lines of the same chapter:

> " 31. Therefore I say: Know the enemy and know yourself; in a hundred battles you will never be in peril.
> 32. When you are ignorant of the enemy but know yourself, your chances of winning or losing are equal.
> 33. If ignorant both of your enemy and of yourself, you are certain in every battle to be in peril."
> (Sun Tzu, 1963, p. 84)

The RMA's focus on "knowing the enemy" entails "...an improved ability to understand target *systems* and their relationship to operational and strategic objectives" because "...knowing *which* subset of targets to strike out of the many identified will be crucial to the effective employment of large numbers of precision weapons." (Krepinevich, 1994, p. 41) "Knowing yourself" is crucial to realizing the RMA goal of "...a major increase in the ability of military organizations to extract the full potential of the human and material resources at their disposal." (*Ibid.*)

II.C. Desert Storm: The Evidence for Third-Wave Warfare

To many writers, the Gulf War clearly demonstrated the military effects of the Information Revolution (e.g., Campen, 1992; Mann, 1994; Mazarr, 1994). Their lines of argument generally proceed as follows. Early suppression and sustained surpassing of Iraq's C3I infrastructure made victory a foregone conclusion. Iraq's limited direct channels for acquiring battlespace data were decimated at the conflict's outset, leaving its "...radar eyes ... poked out, its wireless nerves severed" (Morton,

1995, p. 5). Ongoing aerial reconnaissance was suppressed along with all other Iraqi air missions, and satellite intelligence was denied because commercially available downlinks were controlled by Allied coalition members. Indirect channels (e.g., the public media) were manipulated to mislead Iraq's command into concentrating on the eastern end of the Kuwaiti front (along the Gulf coast). Perhaps the most important aspect of this manipulation was the complete suppression of information hinting at the large Allied buildup in the desert far to the west of what Iraq presumed to be the inevitable front lines. Additional information-oriented factors ranged from the computer-enabled precision of cruise missiles to global media vilification of Sadam Hussein's regime to psychological operations motivating mass desertions and surrenders of Iraqi troops (cf. Waller, 1995).

In the aftermath of the Gulf War, it became apparent that the key success factors were best explained with regard to the acquisition and processing of information, the integration of this information into a base of knowledge, and the conduct of warmaking activities based on this evolving knowledge. Conservatively, Krepinevich appraises Desert Storm as a "*precursor war* -- an indication of the revolutionary potential of emerging technologies and new military systems" analogous to the British success at Cambrai in 1917 (1994, p. 40). The tentative nature of this shift is emphasized by McKenzie (1995), who returns to the Cambrai analogy to point out "...the British Army's unreadiness to exploit its surprise success left it open to an embarrassing reverse in a German counterattack." (p. 20)

The Tofflers (1993) and Mann (1994) take a more expansive line, claiming Desert Storm represented the first "information war" or third-wave conflict in history. They go on to suggest that the Allies' victory was all but inevitable given the disjunction between their third-wave orientation and Iraq's outdated second-wave approach. This third-wave attribution extended beyond command, control and intelligence issues to the weapons themselves. For example, the effective (and cost-effective) usage of cruise missiles in Desert Storm was reinterpreted in terms of applying precise information (e.g., terrain maps, recon photos) to deliver precise effects (maximal destructive effect balanced against minimal collateral damage).

This is not, however, the only possible interpretation. DiNardo and Hughes (1995) criticize such a faddishly RMA-oriented analysis on the basis that it "...grossly overstates the importance of information." (p. 6) They suggest such interpretations are reading much into an event better (and more simply) explained as "...the military

equivalent of 'wish chess' against an opponent accurately described by a perceptive critic as 'a third-class Soviet clone'." (p. 7) This interpretation -- a minority viewpoint -- is constructive in its call for restraint and in its demonstration that Desert Storm was at best preliminary (and not final) evidence for fundamental change in military affairs. These points are, however, more substantively made elsewhere (e.g., Krepinevich, 1994; McKenzie, 1995). The irony is that one might question the finality of the claims from these authors (both academic historians) on the basis of their own closing declaration that academic theorization should be subordinated to empirical evaluation. To judge from the literature, it is military professionals who put the most stock in the concept of an MTR in progress.

II.D. Some Uncommon Themes Relevant to the RMA and IW

The foregoing themes were drawn from the literature of the military community. It should not be surprising that an equally intense interest in information and IT aspects of power and war has been evidenced in non-military circles. This other work is relevant at least with respect to theoretical background, it is voluminous, and it is almost completely ignored by the military community's own publications on IW. Much of this additional literature is associated with current "post-modern" (also "post-structuralist," "critical-theoretical," "deconstructionist") writings in philosophy, cultural studies, communications and media studies, literary criticism, sociology, anthropology, and political studies.

At first glance, one might question the relevance of such "non-technical" or "non-military" work to the field of IW. However, the worldwide penetration of IT -- and the corresponding proliferation of novel socio-cultural phenomena -- provides the background against which IW is delineated. The Tofflers (1993) emphasize that third-wave warfare will bear little resemblance to the well-delineated contests between professional forces that characterized second-wave war. Cyberspace is "everywhere," and warfare utilizing or occupying this non-spatial space will be intimately intertwined with the everyday channels of information flows and subject to the means and manner of everyday information "processing." Phrased another way, IW's battlespaces will be interlinked with (if not contained within) world "culturespaces," and knowledge of these non-military spheres may prove critical for success (cf. Hammond, 1994). Owing to this, socio-cultural studies illuminating the current "Revolution in Social Affairs" are necessarily relevant to understanding

IW prospects and potentials.

This literature is replete with allusions, terminology, and rhetorical tactics which are opaque to the military / engineering communities from which much of the IW literature originates. No comprehensive introduction to this non-military literature will be undertaken in this document. However, the following sections will briefly sketch two critical thematic intersections with IW issues, both of which are overlooked or ignored in the military / engineering literature.

II.D.1. Semiotics: Signs and signification

Semiotics is the field of enquiry into signs, symbols, and the means by which they impart referentiality and / or meaning in use (*signification*). Semiotics is a more abstract endeavor than linguistics, and it is generally considered (at least by semioticians) to subsume the study of natural language as one specific signification system of signs or symbols. Formal semiotic models, such as the triadic model of Charles S. Peirce (1933), make allowance for the interpretation of (or orientation to) the sign being studied. This links semiotics to the sort of cognitive interests pursued in human factors / cognitive engineering studies. Any type of sign / symbol system is a proper subject for semiotic analysis, and the range of such systems analyzed is essentially universal (cf. Eco, 1976, pp. 9-14). In the last decade, IT researchers have increasingly turned to semiotics for theory and frameworks to apply in *human computer interaction (HCI)* areas such as interface design, symbology, etc.

The scope of semiotics has allowed this field to address many of the symbolic phenomena which are manifest in the "information realm" or "cyberspace" (e.g., images, electronic media works, visual rhetorics, virtual realities) which is a focus of IW. Because semiotics seeks to interpret and explain the process(es) by which signs convey meaning, it is relevant to the study of how systems of such signs (e.g., data files, sensor imagery) can be used or manipulated. This can be phrased more directly in a very concise fashion. According to Sun Tzu, "All warfare is based on deception." (1963, p. 66) Umberto Eco (1976, p. 7) declares, "A sign is everything which can be taken as significantly substituting for something else. ... Thus semiotics is in principle the discipline studying everything which can be used in order to lie."

II.D.2. Textuality: the critical role of interpretation

Much "post-modernist" writing is concerned with "texts." To the extent that this work is concentrated in the humanities (especially literature studies), this would seem obvious. What is not so obvious is that (drawing heavily on semiotics) the construct "text" is applied to almost any product of symbolization. Other common terms applied with this broad scope include "narrative" and "discourse." As such, the interpretation of a "text" is a focal metaphor for analyses of all manner of information artifacts. The relevance for IW lies in the fact that these other (apparently tangential) scholarly areas have spent the last two to three decades scrutinizing the interpretation and interpretability of information artifacts. This work highlights the contextual and inter-textual factors which influence the effect or impact that information may have on the interpreter.

Perhaps most relevant at this point in time is the fact that "post-modernist" writers have concentrated on issues of "interests" and "empowerment" in their analyses -- i.e., the manner and the means by which "texts" reflect, impart, or reinforce socio-political distinctions and structures. For example, at a very abstract level, Deleuze and Guattari (1986) critically interpret systems of signification as the primary elements of power manipulation. Virilio (1983) analyzes the diffusion of warfare throughout the media, and thereby throughout the medium, of modern life. Norris (1992) analyzes and criticizes the conclusions (but not the basic critical stance) of post-modernist analyses of the Gulf War. Even more to the point is Der Derian's (1992) survey of the changing face of warfare from a post-modern perspective. These analyses are relevant to IW because:

- they illustrate or analyze systems of socio-political signification already "in play"
- they inform the study of how such systems operate
- (as a dominant "mind set" in Western universities) they are inculcating a "critical attitude" among the practitioners and the targets of future IW.

II.E. Summary: The Current RMA

To summarize, there is widespread acknowledgement that a revolution in military affairs is in progress. The Tofflers and Desert Storm are often invoked in support of the view that this RMA is co-evolving with newly-emergent information technologies and global data / communication networks. Absent a comprehensive modern military theory of informational conflict, Sun Tzu has been resurrected as an exemplar of the warfighting style likely to emerge from the RMA. These three key reference points for the RMA / IW debate each have their imperfections -- the simplicity of the Tofflers' "1-2-3" historical analysis, the ambiguities over what Desert Storm represented, and the largely allusive nature of *The Art of War*. The "cautionary thoughts" of (e.g.) DiNardo and Hughes are just that -- grounds for exercising caution, but not demonstrable invalidations of the notion that an MTR is in progress and that its general character matches the IT-driven RMA vision. We have identified two areas of active scholarly work (semiotics and post-modern textual studies) largely unrecognized in the military community, but specifically addressing the issues of signification and interpretation which underlie information processes.

The key element in the RMA vision is that success in warmaking depends upon the efficient and effective acquisition, synthesis, selection, and employment of information. The broad category of military activities applying this vision is termed IW. The ends and means for this new war form are not effectively addressed with the principles and tactics of industrial (i.e., second-wave) warfare (cf. Jensen, 1994), and new ones must be derived. Beyond this point, the IW picture becomes murky due to differential terminologies, interpretations, and objectives. In the following sections, we shall attempt to sort out this confusing situation on our way to specifying a potential research program in IW.

III. INFORMATION WARFARE (IW)

Like IW, IT has been defined only vaguely -- in some cases subsuming all communications and in other cases restricted to the communication of symbolic data. The former, more comprehensive, definition will be employed in this document, because IW tactics may target both direct interpersonal communications (e.g., telephone calls) and those communications involving data units capable of storage and manipulation (e.g., electronic mail). This allows us to delineate IW with respect to general themes and to avoid some characterizations in the literature which we believe to be overly specific and possibly misleading. In addition, it allows us to follow the more incisive authors in characterizing IW's most novel aspects -- warfighting aimed at the adversary's "beliefs" and "knowledge."

The term *information warfare* has emerged as the label of choice for an ambiguously-delineated assemblage of issues, analyses, and initiatives. By and large, these are aimed at highlighting and addressing the fact that information (in all its forms and functions) is an increasingly critical component of military operations, and that *cyberspace* ("...the global world of internetted computers and communication systems" -- RAND, 1995d) is itself an increasingly important and probable battlespace. The topical scope of IW varies among authors on the subject, with general agreement on core issues and little consensus on its boundaries (Stein, 1995). This ongoing ambiguity has prompted critics to question the viability of the term as a worthwhile construct (e.g., DiNardo & Hughes, 1995). The situation is further complicated by the fact that IW (by anyone's account) significantly overlaps with other topical areas such as *command and control warfare (C2W), command, control, communications and intelligence (C3I)*, and *command, control, communications, computers and intelligence (C4I)*. This document will attempt to itemize the consensus core themes, specify areas of disagreement or ambiguity, and delineate the major potentials and categories of IW at this very early stage of its development. Owing to the volume of novel and often conflicting terminology associated with this area, a glossary is provided at the end of this document.

III.A. Current Interest in IW: Summary of the USAF Perspective

The attention to information warfare can be construed as the military's response to

the global changes wrought by IT. Generally, the notion of transformations in work impelled by the rise of information technologies has been a longstanding theme of speculation and research. As the visions of Vannevar Bush (1945) and Douglas Engelbart (1988a; 1988b) evolved into the marketable commodity of the Internet, analyses and projections of IT's impacts have broadened from individual workplaces to society at large. At this more "macroscopic" level, it has become apparent that the IT Revolution has military ramifications. The impetus for IW research derives from the lessons learned from the 20th Century's technology-intensive wars. Insufficient attention to the ramifications of earlier technologies has contributed to strategic and tactical disadvantage and even defeat. IW analyses are a first step toward avoiding similar disadvantage or defeat with respect to computers and other information technologies (cf. Arquilla, 1994; Cooper, 1995; McKenzie, 1995). This defensively-oriented interest is made all the more important by the fact that the USA (as the most "computerized" nation in the world) is the most susceptible to IW (cf. Dunlap, 1996; Cooper, 1995; Munro, 1991; 1995, Jensen, 1994).

Information warfare has become a key technology of interest to future-oriented defense planners and administrators. Air Force Secretary Dr. Sheila E. Widnall (1995) broadly describes IW as: (1) a possibility "... brought into being by incredible capabilities in processing and disseminating data"; (2) a step "...toward new world vistas, new styles of warfare, and revolutions in warfare"; and (3) a mission which " 'flows naturally' out of assets such as Joint STARS, AWACS, RC-135 Rivet Joint and U-2." Maj Gen Robert E. Linhard, Air Force Director of Plans, sees a potential for effective and efficient force projection of a new sort, "...using information and space-based assets to help influence behavior, decisions and events in an area without physically being there." IW facilitates this because it "...allows us to use the power of information itself to influence the way others may act and exert a real sense of presence." IW is therefore a key element in accomplishing USAF Chief of Staff Gen Ronald R. Fogleman's goals to "provide global situation awareness; dominate the information spectrum; and continue to expand U.S. influence abroad." (Fogleman, 1995b) In pursuit of this potential, Gen Joe Ralston, Vice Chairman of the Joint Chiefs of Staff, specifies the USAF IW objectives as:

- *Controlling the information realm* while protecting our information operations from enemy actions

- *Exploiting control of information* to enhance force employment against the enemy
- *Enhancing overall force effectiveness* by fully developing information operations (Arana-Barradas, 1995)

This has led to a progression of USAF definitions for IW (cf. the Glossary entry on information warfare). Representative of early definitions is the one given in the forecasting document *New World Vistas* (U.S. Air Force Scientific Advisory Board, 1995), which states IW "...has three components. One is the method, or core, of IW which uses computers and software to deceive and destroy enemy information systems. The second component is deployment. Deployment may be as simple as connecting to the Internet, or it may require special communication systems, high power microwave systems, special forces action, or surreptitious individual action. The final component is Defense."

The currently operant USAF definition of IW is "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions." (Widnall & Fogleman, 1995, pp. 3-4) This definition appears stable for administrative purposes, but the full dimensions of IW will likely be subject to ongoing specification (cf. Hammond, 1994; Szafranski, 1995; Stein, 1995).

The next task is to specify the means for IW prosecution. Gen Joe Ralston (Vice Chairman, Joint Chiefs of Staff) has identified three classes of operations as critical to IW objectives, but not suitably addressed by current USAF missions:

- *Counter-Information* to control the information realm
- *Command Control Attack* to subvert or destroy the enemy's command and control system
- *Information Operations* enhancing the employment of military forces through the acquisition, transmission, storage or transformation of information (Arana-Barradas, 1995)

The accomplishment of these (and other tasks) were procedurally categorized in the "functional breakdown" of IW found in the publicly-accessible document entitled *Cornerstones of Information Warfare* (Widnall & Fogleman, 1995, pp. 5-6) as follows:

I. Information Warfare (IW) subsumes actions to:

A. Attack and Defend Information through:

1. *Psychological operations* -- using information to affect enemy reasoning
2. *Physical destruction* (of information systems and networks)
3. *Military deception* -- misleading the enemy about capacities and intentions
4. *Information attack* -- direct information corruption without physical damage
5. *Security measures* -- preventing enemy knowledge of capacities and intentions
6. *Electronic warfare* -- denying the enemy accurate information

B. Exploit Information through:

1. *Information operations* -- "any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces." (*Ibid.*, p. 11)

At the time of this writing, the latest draft statement of U.S. Air Force thinking on IW is to be found in Air Force Doctrine Document 5, entitled *Information Warfare* (Department of the Air Force, 1996). This document introduces a revised "functional breakdown" in which IW is decomposed into two major components -- *counterinformation* and *information assurance*. Counterinformation subsumes those activities which "... establish information control and enable all other activities" by creating or promoting "... an environment where friendly forces can conduct operations with some degree of freedom of action, while simultaneously denying the adversary the ability to conduct those operations against friendly forces." (Department of the Air Force, 1996, p. 4) *Information assurance* "...consists of measures to enhance and protect friendly information and functions." (*Ibid.*, p. 6) These two objectives are the basis for decomposing information assurance into the subcategories of *information enhancement* and *information protect*, respectively (*Ibid.*, pp. 7 ff). This latest USAF IW taxonomy is illustrated in Figure 1.

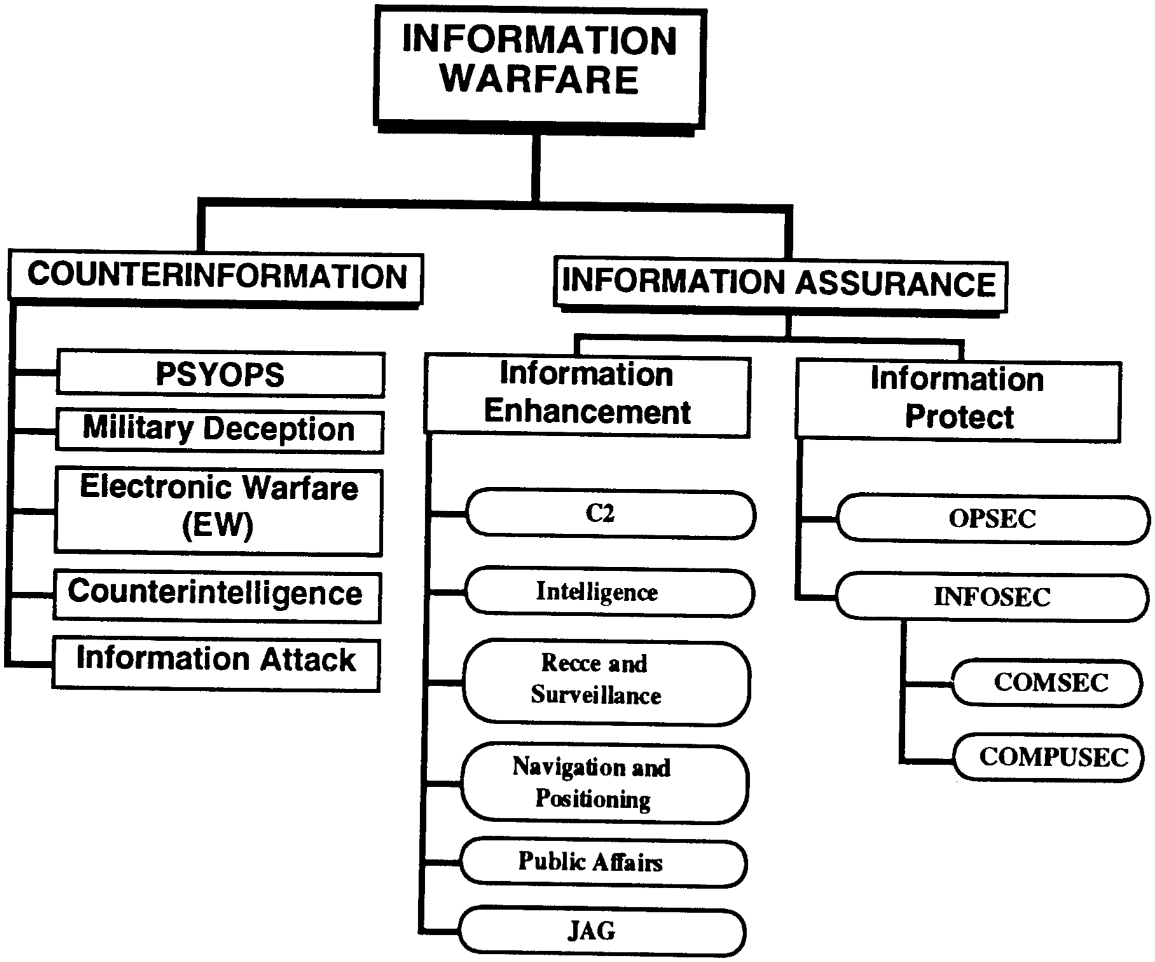

Figure 1: Taxonomy of IW Activities
Source: Department of the Air Force (1996, p. 3, Figure 2-1)

At this point, we are in a position to outline the work reported in the remainder of this document with respect to the current state of USAF formulations. With respect to *Cornerstones of Information Warfare* (Widnall & Fogleman, 1995), this document will outline an approach to USAF IW operations concentrating on Information Operations as the means for launching, in effect, continuous virtual Command-Control Attacks (cf. Ralston) to exploit *information dominance*. With respect to the taxonomy of Figure 1, our focus will be within that area termed Information Enhancement. Command-Control Attack, in the sense of instrumental action against information networks themselves, is an important auxiliary activity lying largely outside the scope of this discussion. This concentration on information operations is consistent with our target application area (theater attack operations).

Information operations is the area most closely linked to changes deriving from the

RMA. Achieving the above-listed IW goals requires integration and coordination among all elements of the theater system-of-systems. Such an effort is qualitatively different from traditional DOD development and procurement efforts, which have tended to focus on individual technical systems in isolation. "The major management problem facing the Pentagon is focusing on *organizational metrics* rather than on *technical systems characteristics*. ... The objective is the payoff from these changes, which should be judged not in purely technical ways, such as higher data rates, but rather in improvements in organizational performance such as increased responsiveness and efficiency." (Bracken, 1995, pp. 72-73) Process and performance gains are the objectives Widnall and Fogleman (1995) have laid out for information operations.

This does not mean that information operations are purely of administrative interest. IW, like any other innovation in warfighting, entails both offensive and defensive measures (cf. RAND, 1995a; 1995b; 1995c). *Offensive information warfare* tactics "...will degrade or exploit an adversary's collection or use of information," and *defensive information warfare* tactics will aim to "...protect our ability to conduct information operations..." (Joint Chiefs of Staff, 1996, p. 16). The current interest in IW is largely motivated by the fact that the USA's technological lead in IT positions it at an advantage in exploiting IW's offensive potential. By the same token, American and NATO reliance on computers and data networks makes them tempting targets for these same tactics (cf. Berkowitz, 1995; Cooper, 1995; Tigner, 1995). The majority of writings on defensive IW concentrate on the defense of information systems (e.g., from viruses and unauthorized hacking), which lies outside the scope of our consideration (as a component of "security measures" as defined above). However, Dunlap's (1996) "horror story" of American defeat by a third-world adversary plays heavily on US vulnerabilities to media manipulation, deception, and propaganda exploited outside the venue of computer networks and largely outside any conventional physical battlespace. Information operations can be construed as "defensive" to the extent that it establishes and maintains own-system integrity in the face of adversary actions.

Finally, information operations is the component of current USAF IW doctrine which is maximally exploitable where there is "asymmetry" in conflict -- the differential between capacities, intentions, and tactics between dissimilar combatants (e.g., between guerrilla insurgents and professional military forces). Dunlap's (1996) pessimistic fictional scenario derives in large part from a projected

presumption that IW would always involve computers and data networks. The fictional third-world victor obtained tactical advantage by avoiding such technological channels, making its operations "invisible" or "opaque" to a sophisticated, but computer-centric, American military establishment. IW innovations in own-system operations will be viable in both symmetrical and asymmetrical conflicts. Therefore, a concentration on information operations is a constructive direction for research and development with maximally-exploitable payoffs.

III.B. IW's Ambiguous Boundaries

In the literature, reference to the above-listed themes is uniform in tone but not in occurrence. For example, Jensen (1994) states that IW is best explained with reference to the Tofflers' work and is not effectively addressed from a second-wave perspective, while Mann (1994) outlines IW in terms of what worked in Desert Storm. Beyond references to the three themes, there is little agreement in defining IW. Many authors define IW by allusion, and others by enumeration of specific tactics or settings for action. Figure 2, based on the work of Martin Libicki at National Defense University (cf. Libicki 1994; 1995), is the single most comprehensive illustration of the various activities lumped together under the label "information warfare."

Figure 2 surveys a range of activities subsumed within the purview of IW. As such, it helps in establishing the scope of IW concerns. However, aside from the dichotomy between military and civilian targeting, this layout provides no categorization criteria for differentiating among the activities listed. In a later illustration (Institute for National Strategic Studies, 1996), Libicki's survey layout is enhanced with a second dichotomy -- actions against people versus actions against systems. The result is summarized in Figure 3. This enhanced diagram is more useful than its predecessor for categorizing the diverse elements of IW, but its criteria of differentiation still seem suboptimal. For example, this classification implies that psychological warfare is primarily directed against civilians and electronic warfare against military forces. This apparent breakdown does not account for (e.g.) the use of psyops against Iraqi ground troops in the Gulf War (cf. Morton, 1995; Mann 1994).

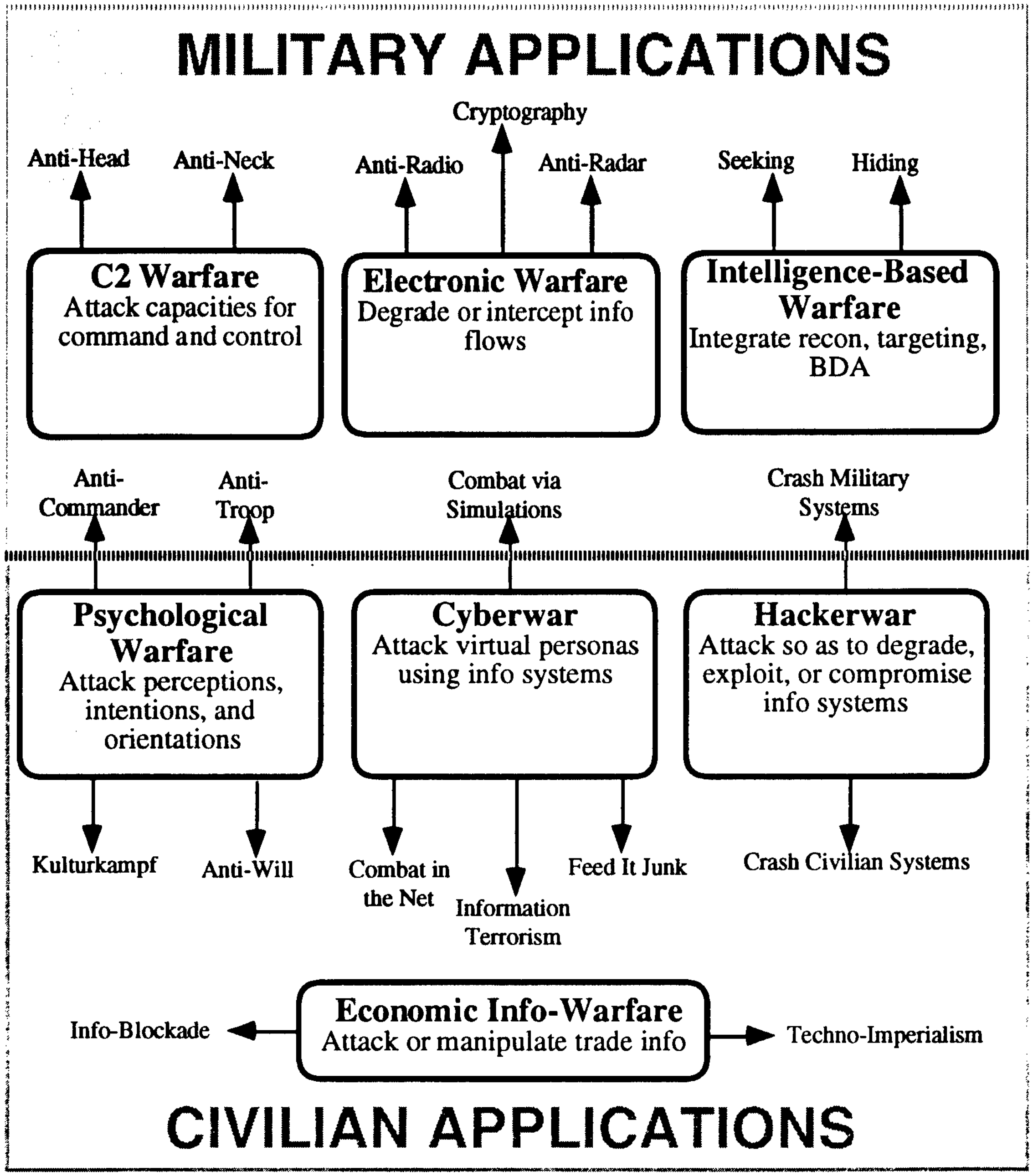

Figure 2: The Range of IW Activities (based on Libicki, 1995)

Attempting to improve upon Libicki's groundbreaking work will require a reappraisal of how IW is delineated and defined. This, as it turns out, is a major task. Authors place IW at diverse levels of generality and define it in terms of divergent foci. In the remainder of this section, we shall attempt to sort through all this diversity and achieve as much coherence as is feasible. The first issue is that of scope -- just how much does IW denote?

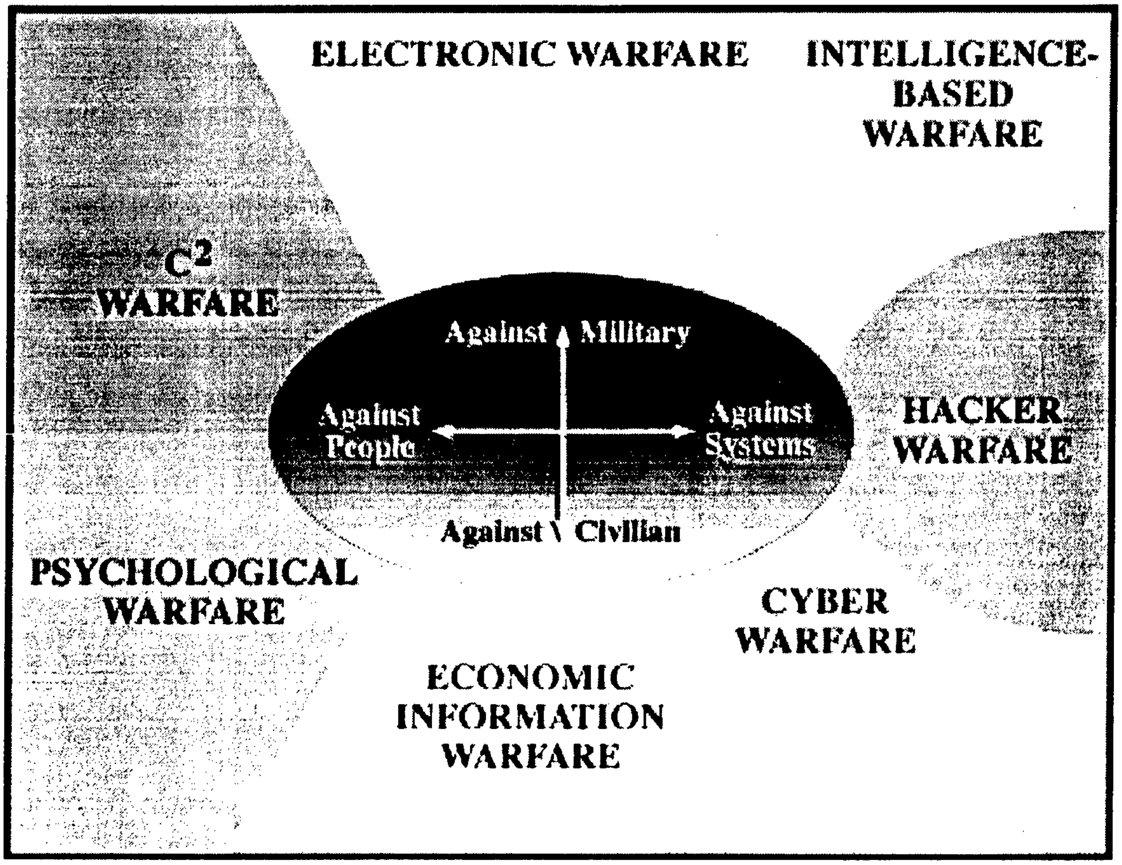

Figure 3: An Enhanced Version of Libicki's IW Taxonomy (Based on Institute for National Strategic Studies, 1996, Chapter 15)

Some seem to see IW as the most general term of reference in addressing warfare involving information. Stein (1995, p. 32) claims IW "...in its largest sense, is simply the use of information to achieve our national objectives," as well as "the emerging 'theater' in which future nation-against-nation conflict at the strategic level is most likely to occur..." This theater of operations will be situated in "...the worldwide internetted and interconnected means of information and communication." Such operations "... may permit the United States to accomplish some important national security goals without the need for forward-deployed military forces in every corner of the planet." In terms of focus, Stein says IW "...is about the way humans think and, more importantly, the way humans make decisions." Such broad strokes depict IW as everything to everyone.

In contrast, Szafranski delineates IW as a particular activity which "...can be prosecuted as a component of a larger and more comprehensive set of hostile activities -- a netwar or cyberwar -- or it can be undertaken as the sole form of

hostile activity." (1995, p. 58). Szafranski's more general *cyberwar* or *netwar* approximates Stein's IW. Szafranski limits his usage of the term IW to "...hostile activity directed against any part of the knowledge and belief systems of an adversary." He therefore distinguishes IW as the subcategory of cyberwar "...that attacks information systems directly as a means to attack adversary knowledge or beliefs." Szafranski's specificity is limited to this subcategory, as he does not separately define either "netwar" or "cyberwar." Attempting to pin down these more general terms leads once again into a terminological morass. "Cyberwar" has been a RAND Corporation synonym for *information warfare* in general (Grier, 1995, p. 37), as well as a term for informational warfighting in the context of official military actions (Arquilla & Ronfeldt, 1993). "Netwar" has been used as a generic label for conflicts waged within computer networks, and more specifically for informational conflicts waged in social (as opposed to military) venues (Arquilla & Ronfeldt, 1993).

The above examples are but a few of the many in the literature, and the reader is referred to the Glossary to review and compare the competing terminologies. It is clear that IW, as a label, has been stretched to fit a number of different scopes. The net result is that the label has lost any explanatory power except as a generic descriptor for warmaking involving information and information systems. For the purposes of this discussion, we shall take IW to be a general term, and we shall follow Gen Joe Ralston, Vice Chairman of the Joint Chiefs of Staff, in defining it as:

> *"... any action to deny, exploit, corrupt or destroy the enemy's information and its systems; while protecting against those actions; and exploiting our own information operations. "* (Ely, 1995)

This definition still allows for a number of divergent foci. To some authors IW "...means the emergence of greatly improved methods of command, control, and communications." (Grier, 1995) Nonetheless, it is difficult to relate IW to earlier constructs such as (e.g.) *command, control, communications and intelligence (C3I)* and *command, control, communications, computers, and intelligence (C4I)*. These terms pertain to the elements participating in the *(infra-)structure* within which command and control is effected. Actions relating to these constructs (e.g., *command and control warfare -- C2W*) prioritize these (infra-) structures as objects of manipulation, e.g., using "...physical and radio-electronic combat attacks against

enemy information systems to separate enemy forces from enemy leadership." (Szafranski, 1995, p. 65, footnote 1)

IW, on the other hand, "...is fundamentally not about satellites, wires, and computers" (Stein, 1995, p. 32), but about command and control *functions*. Szafranski (1995, p. 65, footnote 1) claims IW surpasses C2W's structural focus by being "...a much larger set of activities aimed at the mind and will of the enemy." Prior constructs have characterized adversaries in terms of their (infra-) structures, prioritized degradation of such structures as ends, and concentrated on manipulations of such structures as means. This approach makes *cyberspace* ("...the global world of internetted computers and communication systems" -- RAND, 1995d) both the battlefield and the object of battle. In IW, acting against information systems (and their associated communications assets) is but one means for attacking the adversary's ability to interpret, understand, and act. As Stein (1995, p. 33) puts it, "Cyberspace may be the new 'battlespace', but the battle remains the battle for the mind. There must be no confusion of the battlespace with the battle."

Unfortunately, much of the IW literature fails to overcome this confusion. We must therefore sort out these confounded notions to provide a focused view of IW. For the purposes of this analysis we shall reserve the terms C2, C2W, C3I, C3W, C4I, and C4W to denote activities aimed at leveraging the structures of command and control. With respect to the "information realm," these structures comprise the *vehicle(s)* or *media* via which command, control, and intelligence functions are accomplished. Offensive and defensive actions directed at such structures will hereafter be collectively referenced as *information systems warfare (ISW)*.

Separating out ISW allows us to focus more clearly on the other side of the IW coin -- those actions aimed at leveraging the *contents* and derived *products* of these media. Offensively, such actions seek to affect the "...the mind and will of the enemy," as Szafranski puts it. Defensively, they facilitate one's own "mind" (capacity for command and control) and "will" (resolve and decisiveness). These complementary "mind and will" activities will hereafter be collectively referenced as *information dominance warfare (IDW)*. IDW operations are directed toward command, control, and intelligence functions, regardless of the precise structures through which these functions are conducted. In effect, the ISW / IDW dichotomy is a re-framing of the "people vs. systems" dichotomy in Figure 3 to more accurately reflect the position that although the ultimate target of IDW is ultimately people, the

immediate target of IW activities is the information which those people engage. This referential shift portrays the "people / systems" dichotomy in such a way as to more clearly maintain focus on own-system capacities and venues of tactical engagement.

It should be clear that these two categories of warmaking are often interlinked in practice. For example, IDW may employ ISW to either corrupt the adversary's knowledge base repository or to deny him access to all but those information channels which are subject to IDW manipulation. Conversely, IDW tactics diminishing the adversary's confidence in his information systems may serve an ISW agenda. Nonetheless, these two concepts must be considered separate, because achievement of one is not necessary to achievement of the other. We shall use the ISW / IDW distinction to integrate the jungle of IW connotations into a unified categorizational scheme. Before we can do that, however, IDW's fundamental concept of *information dominance* will require further elaboration in the next section.

III.C. Information Dominance

Sun Tzu's "acme of skill" connotes the ability to subdue an adversary without destroying him, hopefully without having to engage him in lethal combat. The Tofflers (1993) repeatedly emphasize that in third-wave war victory will be judged in terms of eventual effect rather than degree of destruction. This is reflected in Jensen's (1994) prescription of a shift from "deterrence theory to inducement theory" and Hammond's (1994) vision of future warfare aimed at changing perceptions. Such subjugation is a matter of directed influence, and the measure of success in exercise of such influence is dominance over the adversary.

The term *information dominance* is often used to connote ongoing relative advantage attributable to IT and utilization. According to Lee (1994), the concept dates back to Soviet military theorists of the late 1970's. They were assessing the ramifications of the USA's technological superiority in IT -- a superiority considered to constitute an MTR(cf. Krepinevich, 1992, p. 14). The projected outcome (information dominance) was "..a condition in which a nation possesses a greater understanding of the strengths, weaknesses, interdependencies, and centers of gravity of an adversary's military, political, social, and economic infrastructure than the enemy has on friendly sources of national power." (Lee, 1994, p. 3; cf. Krepinevich,

1992, p. 22) The most recent statement of this theme uses the label *information superiority* to denote "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." (Joint Chiefs of Staff, 1996, p. 16)

In a similar vein, Mann (1994) equates information dominance with relative advantage in information collection, dissemination, and application. He characterizes these activities as facilitating and feeding a base of knowledge (distinct from information) upon which tactical decisions are then made, and conventional action is undertaken on a physical battlefield. Others (e.g., Hammond, 1994; Szafranski, 1995; Jensen 1994) set as a clear goal the achievement of a dominance in the information realm analogous to (but separable from) physical dominance on the traditional battlefield (whether or not they use the term "information dominance"). Hammond and Szafranski, in particular, prioritize dominating enemy perceptions, beliefs, and knowledge over secondary effects on the physical battlefield. This prioritization reaches an extreme in Ryan (1995), who claims that IW will not only determine conventional military outcomes, but may come to be seen as the basic war form of which armed conflict is but the final stage. Libicki (1995) employs the term more with respect to IT itself, to connote that "One side's information systems may be better (more powerful, robust, and reliable) than another's."

More concretely, Owens (1995a; 1995b; 1995c) outlines three basic ensembles of systems contributing to an operational *system of systems (SOS)* architecture for information dominance:

• *Battlespace Awareness.* This is the system for data and information acquisition (e.g., via sensors) through which one develops and maintains awareness of the battlespace and all parties operating within it. Battlespace awareness is facilitated by efficient and effective surveillance, reconnaissance, and intelligence operations.

• *Advanced C4I.* This is the system "...that converts the information derived from battlespace awareness into deeper knowledge and understanding of the battle space..." and in turn "...converts the understanding of the battlespace into missions and assignments designed to alter, control, and dominate that space." (Owens, 1995a, p. 38) Advanced C4I is facilitated by efficient and effective data fusion, analysis, planning, and decision making.

• *Precision Force Use.* This is the system in which action is realized, using the information and knowledge fed forward from the first two systems to maximize force application while minimizing adverse collateral effects. This concept focuses on the use of information and knowledge to improve force projection, and not on the automation of warfighting per se (cf. the *hyperwar* concept of Arnett, 1992). Precision force use is facilitated by increasingly refined specifications for action (tactics, orders) and sophisticated means for enacting those specifications.

The SOS and its three constituent subsystems are subject to optimization with respect to parameters of cost, resources, and performance. This provides the basis for applying techniques from (e.g.) systems analysis, operations research, and human engineering. Battlespace awareness is optimizable through enhancing data capture (e.g., better sensors, wider sensor coverage) within cost and resource constraints such as platform prices, attrition risks, and logistical limitations. Advanced C^4I is optimizable through improved transformations of data into information and knowledge (e.g., data fusion, intelligence analyses), as well as enhanced application of these results to decision making (e.g., decision support systems). This entails trade-offs against cost and resource constraints such as bandwidth, time pressure, and information processing capacities. Precision force use is optimizable through improved transformations of decisions into instrumental actions (e.g., weapons delivery, targeting) while minimizing cost / resource factors such as own-force attrition, casualties, fratricide, and collateral damage.

By grounding the idea of information dominance in these three systems, Admiral Owens makes it possible to map the concept onto specific operations and players. Owens' framework illustrates how dominance can arise by sustained advantage at all points along the path of feed-forward from reconnaissance to response. This links information dominance to success within and among these systems, and provides a basis for addressing the basic capabilities which would promote information dominance in an actual theater of operations. Owens (1995b) lists four such basic capabilities:

• *200 x 200 nm area of responsibility.* This capability circumscribes an *extent* of dominance relative to the spatial extent of the theater battlespace.

• *Day / night, all-weather coverage.* This capability circumscribes a *continuity* of dominance activities corresponding to the ongoing threat potential in the theater of operations.

• *Near perfect information.* This capability prescribes a standard of *quality* for the focal product of dominance activities (i.e., information). Note that this "quality" is apparently delineated with respect to the product itself -- i.e., in terms of "timeliness, specificity, and accuracy." (Widnall & Fogleman, 1995, p. 1).

• *The right information to the right warfighter at the right time.* This capability prescribes a standard of *effectiveness* in leveraging the focal product (information) to achieve dominance. Note that "right information" connotes "quality" in a different sense than in the preceding point -- i.e., appropriateness relative to a specific warfighter in a specific situation within the theater of operations.

Owens' vision of information dominance capabilities links the operational architecture (i.e., the three systems) to battlespace parameters and tasks. It qualifies information dominance with respect to specifics of setting, players, tasks, and results. We believe this pragmatic focus is the key to applying abstract IW concepts in real-world USAF operations. For the purposes of this discussion, we shall define information dominance in a given theater of confrontation, and in relation to a given adversary, as:

an operational advantage obtained through superior effectiveness of informational activity (acquisition and processing of data, information, and/or knowledge), to the extent that this advantage is demonstrable through superior effectiveness of instrumental activity.

This definition differs from those explicit in the IW literature by virtue of the fact that it demands a linkage between superiority of informational activity and superiority of instrumental activity. To the extent that instrumental superiority derives from leveraging information and knowledge, the advantageous effect is *information* dominance. This definition therefore excludes advantage conferred by *instrumental dominance* in and of itself (e.g., overwhelming firepower). On the other hand, it is only to the extent that information is leveraged to obtain superior instrumental action

that *dominance* is effected. The definition therefore excludes any apparent informational advantage in the theater of confrontation which results in no effect, or even a negative effect. Amassing a superior base of irrelevant data illustrates "no effect," and information overload illustrates "negative effect."

Phrased another way, this definition does not apply when one merely stops at the point of achieving "dominating" information assets (cf. Admiral Owens' "near-perfect information"). In this definition information dominance requires that: (a) the information is "right" for a specific mission by any (of a class of) warfighters in the theater of operations, and (b) that the systems managing that information make it available to warfighter(s) most "right" for exploiting it. By demanding this linkage between the informational and the instrumental, we are grounding the current (largely figurative) IW discourse in such a way as to pursue tangible operational payoffs.

As time goes on, newer terminology is shifting the focus from the own-system / adversary duality to the own-system characters or features which are associated with information dominance. One such term is *dominant battlespace awareness (DBA)*, which connotes superiority with respect to Owens' "battlespace awareness." The concept of DBA generally focuses on the means for linking together sensor / reconnaissance / intelligence channels for broader and deeper "perception" of the battlespace (cf. Lum, 1994). More recently, this term has given way to the more general *dominant battlespace knowledge (DBK)* (cf. Johnson & Libicki, 1995), which connotes own-system capacities for integrating inputs from battlespace awareness into extant "knowledge of" the theater and "know-how," so as to afford own-system operational "intelligence" -- "...namely, the ability to *understand* what we see and *act* on it decisively" (Rokke, 1995, p. ix). The closest thing to a specific definition of DBK in the Johnson and Libicki volume is given by Alberts (1995, p. 80): "The ability to approach total situation awareness and prevent our adversaries from achieving it, and our capability to exploit our relative advantage in information result in a situation in which we have achieved DBK."

The notion of DBK therefore extents the idea of superiority throughout the entirety of the SOS. Alberts' definition incorporates DBA ("total situation awareness") and information dominance ("relative advantage in information") with a potential for improved action ("capability to exploit"). This definition pinpoints DBK as the feature linking awareness and informational advantage to enhanced effectiveness of

instrumental activity. It should be pointed out that this does not mean that DBK replaces either of the other two terms. Both DBA and DBK are defined with respect to own-system attributes or capacities, and are therefore not isomorphic with "information dominance," which addresses advantage relative to an adversary. Unfortunately, the literature tends to focus on one or the other in such a way as to suggest it supplants the others. For our purposes, we shall reserve the term "information dominance" as a descriptor for own-system / adversary general comparison and apply DBK to connote that quality or capacity of one's own SOS which facilitates information dominance.

Having thus defined and distinguished information dominance, we can now go back to our distinction between ISW and IDW to lay out our integrated reformulation of the multifaceted IW field. This is illustrated in Figure 4. By employing the ISW / IDW distinction, then differentiating between offensive and defensive applications, we are able to sort out the diverse areas and specialties in a more structured manner than even the best such prior categorizations (cf. Figures 2 and 3). To illustrate this, we have classified Libicki's elemental tactics (cf. Figure 2) with regard to this new schema.

Our vehicle / content dichotomy improves upon Libicki's "people vs. systems" differentiation by shifting the "people" aspect to the information directly affected by IW operations. Our offense / defense dichotomy improves upon Libicki's "anti-civilian vs. anti-military" differentiation by prioritizing mode of action rather than socio-political affiliation. This allows our categorization schema to avoid the problematical blurring between purely civilian and purely military aspects of (e.g.) *operations other than war (OOTW).* Having accomplished this, we can now close our analysis of the current state of IW theorization.

	INFORMATION SYSTEMS WARFARE (ISW)	INFORMATION DOMINANCE WARFARE (IDW)
OFFENSE	• Anti-head attacks • Anti-neck attacks • Jamming • Hackerwar (crashing systems) • Info systems blockade • Physical disruption (networks) • Physical destruction (info processors; comm. links)	• Cryptography (codebreaking) • Psychological warfare • "Information terrorism" • "Feed it junk" • Info flow blockade • Deception • Propaganda (offensive 'spin') • Recon / Surveillance (seeking) • Intelligence gathering • Intelligence analysis
DEFENSE	• Maintaining technological edge • Security measures (anti-intrusion) • Stealth • Network communications integrity (anti-disruption) • Anti-virus / anti-hacking measures • Physical protection (anti-destruction)	• Cryptography (encryption) • Psychological warfare • "Information terrorism" • "Feed it junk" • Message blockade • Message camouflage • Media management (defensive 'spin') • Recon / Surveillance (hiding)

Figure 4: IW Categorized in Terms of ISW versus IDW

III.D. Summary: Information Warfare (IW)

In the foregoing section we have surveyed the emergent area of IW. This field is as yet vaguely-defined, even though there is general consensus on the kinds of missions and tactics which fall under its aegis. We have taken the set of candidate activities subsumed under IW and categorized them with respect to (a) offensive and defensive intent as well as (b) the distinction between actions against information systems (*ISW*) and actions against information content and signification (*IDW*). This two-way differentiation permits us to address the area with more precision than most of the literature to date. This categorization should permit us to maintain a clarity of referential focus as this field continues its evolution. In Section IV. we shall proceed to a discussion of the foci and means by which cognitive engineering expertise can be constructively brought to bear on IW issues.

IV. COGNITIVE ENGINEERING AND IW

In this section, we shall delineate and discuss those issues critical to constructive cognitive engineering research on IW issues and needs. First (in subsection A.), we shall discuss the methodological reorientation(s) necessary to address third-wave warfare issues. Next (in subsection B.), we shall discuss the three key topics which cognitive engineering research must address to improve SOS decision processes. In subsequent sections we shall specify a class of solutions as the goal for such research and introduce a novel model as the means for pursuing this goal, and outline an integrated program of cognitive engineering techniques suited to mission and task analyses from an IW perspective.

IV.A. Methodological (Re-)Orientation

As discussed earlier, cognitive engineering is the application of cognitive sciences to the design and construction of information systems that engender effective interaction between the artifacts and the people they support. The goal is generation and introduction of appropriate end user models in the total system design. With respect to IW, two fundamental (re-)orientations are necessary to achieve this cognitive engineering goal -- one pertaining to that portion of IW's purported scope most amenable to cognitive engineering work, and the other pertaining to that portion of specific USAF applications (e.g., TMD BMC4I) most critical from an IW perspective.

IV.A.1. (Re-)Orientation #1: Prioritize IDW over ISW

Information warfare subsumes a number of different connotations, and various writers have placed one or another specific "spin" on the term. As Figure 4 illustrates, we make a primary categorical distinction between (a) warfighting directed at information systems themselves (ISW) and (b) warfighting directed at the information conveyed and processed via such systems (IDW). This latter category is the proper focus for cognitive engineering research. This restriction is straightforward. ISW issues are most properly seen as technical or engineering topics lying outside the scope of human factors, whereas IDW falls squarely within cognitive engineering's domain of expertise. IDW comprises the "side of the equation" on which the humans and their information processing abilities appear, and cognitive engineering is by definition a field concerned with human acquisition,

processing, and employment of "information." From a programmatic perspective, this focus is further justified by the fact that 6 of the 7 IW subcategories delineated in the primary USAF position statement to date (Widnall & Fogleman, 1995 -- cf. p. 5) are cited and discussed as IDW activities. Only the category of "physical destruction" (of data and/or information systems) falls squarely within the area of ISW. In other words, the extent of USAF programmatic interest in the means and manner of protecting, attacking, and manipulating information systems for tactical advantage (i.e., ISW) is limited to only a fraction of the IW "map."

IV.A.2. (Re-)Orientation #2: Prioritize interactional performance

The first reorientation concerns scope of analysis with respect to the actors. To date, most IRA work has been geared toward individuals (e.g., pilots) or small co-located teams (e.g., flight crews) -- a level of "granularity" considerably finer than that required for assessing (e.g.) theater command and control. The most novel aspects of IRA's for such operations will be that they must coherently address performance of the collective, as well as individual, actors.

Information dominance is an advantage defined with respect to a subject versus an adversary. In third-wave conflict, the subject and the adversary are composite SOSs. Accordingly, information dominance can only be evaluated at the level of the entire system(s). Research issues involving *individual* actors (e.g., sensor operators), task performance (e.g., measures of effectiveness), task features (e.g., visual display characteristics), and task events (e.g., target detection) can already be addressed with current cognitive engineering techniques. However, limiting the research agenda to such individuated factors will prove problematical in the long run. Research results keyed to such individuated foci will necessarily be of narrow applicability. Phrased another way, compartmentalization of research issues can only lead to tightly-compartmentalized payoffs. Such research cannot address the scope of current and prospective operations architectures involving hundreds of actors distributed throughout an entire theater (e.g. TMD BMC4I).

Addressing such operations architectures will entail analyses of large, complex, and distributed "systems of systems." It is at the level of these composite systems that IW is being discussed and addressed (cf. Owens, 1995). This overarching behavior cannot be directly discerned or predicted based on the behavior of isolated subcomponents. In broadening the scope of research to the scale of current and prospective SOS architectures, it is necessary to conduct cognitive engineering

within a framework permitting collation and application of results with respect to issues of coordination between the subjects studied and the broader SOS within which they participate. This means that maximally constructive research will be directed toward (a) the relationships between "individual subsystem" and "system of systems" and (b) the functional trade-offs relevant to these relationships. This inter-component orientation has two major aspects -- the first concerning the structure or topology of the SOS information infrastructure, and the second concerning the activities conducted within it. We shall briefly discuss these two aspects and point out the methodological adjustments required for effective cognitive engineering research on IW.

The primary focus of such research is information exchange and processing among the units comprising the SOS. The "information network" linking these units comprises the functional skeleton for the composite. Both literally and figuratively, this network constitutes an *intermedium* lying between and among individual actors and their collective units (cf. Figure 5). The literal intermedium is made up of (e.g.) cables, computers, and over-the-air communication links. The figurative intermedium is made up of (e.g.) shared data and messages. Offensive and defensive IW tactics are played out within this intermedium, with individual actors / units being targeted only indirectly (cf. Widnall & Fogleman, 1995, pp. 6-7). Research focusing on individual actors and their performance will naturally remain important, but exclusive attention to such individual issues will necessarily fail to address the intermedium where IW is operant.

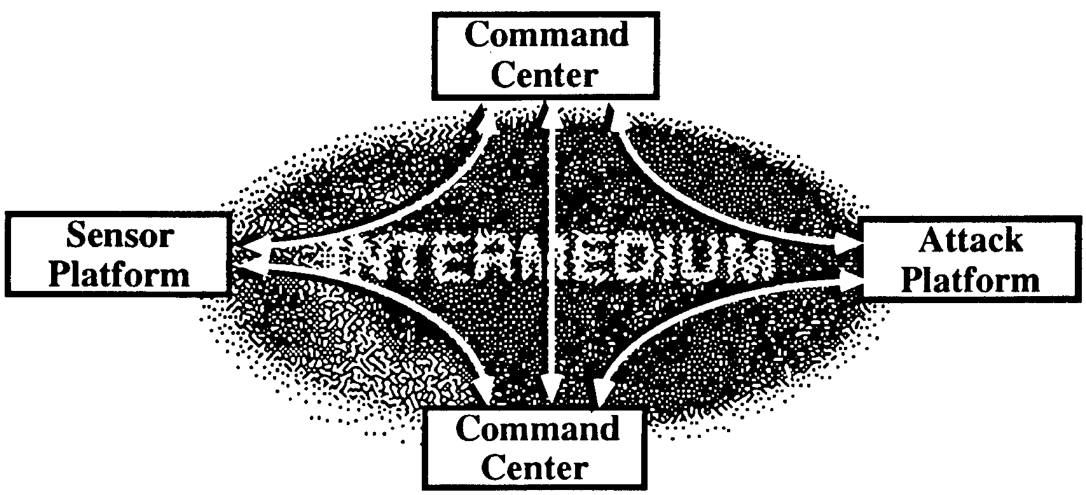

Figure 5: The Intermedium Integrating the System of Systems

The second aspect of the inter-component orientation concerns activities. The networked SOS is effective to the extent that its subcomponents jointly contribute to the overall mission. It is the interaction among these subcomponents which determines the extent to which the "whole" falls short of, equals, or exceeds the "sum of its parts." Because this interaction is conducted within and across the domains of diverse information systems, it is also the critical activity for offensive and defensive information warfare strategies. Prior cognitive engineering work has generated expertise, experience, and diverse means for addressing SOS informational and functional aspects through (respectively) *information requirements analyses (IRAs)* and *task analyses.* However, prior instances of such analyses have concentrated on single operators and/or single systems. IW's necessary shift in scope from individuals to intermedium requires a corresponding shift in analytical methodology. The first, and most basic, step toward this shift is to lay out those features or factors most critical to performance in the intermedium.

Additionally, the most obvious types of previous human factors / cognitive engineering research carried forward into the IW / SOS realm -- situation awareness and decision making -- must be approached with regard to (e.g.) "shared situation awareness" and "team decision making." This does not require abandoning the general theories and methodologies previously applied in these areas. It requires only that the application of such theories and methodologies (a) be adapted to address multiple actors working in tandem and (b) be applied with primary regard to the intermedium through which this collaboration is realized.

The methodological adjustments introduced here are research issues in and of themselves. A viable research methodology and toolkit addressing the intermedium would constitute a novel product positioning the USAF to more effectively assess and exploit IW aspects of the trend toward larger and more complex system-of-systems deployment and operational styles.

IV.B. Key Topics for Cognitive Engineering Research

In subsequent sections, we shall:

- Specify a class of solutions for current IW needs (*common battlespace displays*)
- Introduce an integrative model for addressing these needs from a cognitive engineering perspective (the *OODA Model*)
- Delineate a comprehensive cognitive engineering program meeting current USAF needs

First, however, we must sort out the problematical aspects of addressing IW with current cognitive engineering tools and techniques. This section will accomplish this by more deeply discussing the three cognitive engineering adjustments prescribed in the last section:

(a) SOS interactional foci for cognitive engineering research
(b) Situation awareness in distributed collaboration networks
(c) Decision making in distributed systems of systems.

IV.B.1. Intermedial factors affecting interactional efficiency and effectiveness

The question arises as to how to assess prospective research activities in planning an effective IW agenda. The best criteria for such assessments will be critical performance factors in the application area. Having reviewed the research in relevant fields (e.g., *computer supported cooperative work (CSCW), human-computer interaction (HCI),* and *computer-mediated communication (CMC)*) we have laid out a set of six such factors specific to collaborative interaction via distributed information systems. Because these pertain to performance within and across the intermedium, they will be termed *intermedial factors*. The remainder of this section will briefly discuss these intermedial factors and indicate the means by which they may be addressed.

1. *Connectivity among SOS actors needing to confer and collaborate.*

This factor relates to the ability of actors to communicate as much, as long, and as frequently as is necessary for optimal SOS performance. Although connectivity is certainly an important factor (in the literal, physical sense) for ISW, it is also critical (in the figurative, procedural sense) for IDW. This means that physical, logical, and temporal factors are properly considered connectivity topics to the extent they address accessibility in and of itself (cf. "coordination" on temporal factors). Connectivity-oriented studies might address (e.g.) necessary, sufficient, and alternative lines of access to information flows, degree of flexibility in switching channels, and the like.

2. *Consistency of information and information flows in the networked SOS.*

This factor relates to the relative correspondence of information units ('raw' or

processed) between actors. Phrased another way, consistency relates to stability of informational form and / or content across the population of relevant actors. Research on consistency could, for example, identify bottlenecks and translation delays, analyze their effects, and prescribe solutions for improved performance. Another example would be assessments of distributed operators' ability to jointly orient themselves (with different data displays) with respect to a commonly-referenced object (e.g., a target).

3. *Comprehensivity of information available to actors in the SOS network / chain.*

This factor relates to the relative 'completeness' of the information available to either a particular SOS unit or the SOS as a whole. Phrased another way, comprehensivity relates to the scope of information available to a population of relevant actors. Information requirements analyses could lay out the necessary, the sufficient, and the optimal information factors for individual SOS nodes and the SOS as a whole. Examples of research issues related to comprehensivity include informational sufficiency, dataflow requirements, decision making under uncertainty, and reasoning with incomplete data.

4. *Comprehensibility of information flowing through the SOS network.*

This factor relates to the ability of actors to receive, transcribe, translate, interpret, and employ incoming data units. Phrased another way, comprehensibility pertains to an actor's ability to make sense of or recognize an informational item. Comprehensibility relies on other factors such as consistency and congruence, but it is not reducible to them. Examples of comprehensibility-oriented topics include signal detection, image recognition, and message disambiguation.

5. *Congruence of information and information flows in the SOS network.*

This factor relates to the relative fit of information units with each other or with respect to an overall perspective on the task. Where comprehensibility is a feature of a given informational item in and of itself, congruence is defined in terms of interrelationships with other such items. Consistency is a feature of informational similarity among multiple actors, and comprehensivity is a feature of informational scope with respect to a topic or purpose. In contrast, congruence is a feature of informational synergy for any actor. Phrased another way, congruence pertains to the degree to which data and information units can be "added up" to achieve a state of focused situational awareness. Studies focusing on congruence might address (e.g.) the degree to which multiple data streams or information items may conflict

before spoofing is suspected, evaluations of situation awareness from fused data streams, and the like.

6. *Coordination of information and information flows among SOS actors.*

The term "coordination" is used here in the strict sense of managing the patterns of dynamic change in the SOS information network (as opposed to the senses synonymous with "consistency" and "congruence" as defined above). Coordination (due to its focus on dynamics) is also distinct from temporal and logical aspects of "connectivity" (which focuses on accessibility). Coordination-oriented studies might address (e.g.) the temporal issues of pacing and sequencing network information flows.

Examples of Research Addressing the Six Intermedial Factors

In keeping with the system-wide viewpoint emphasized above, studies of these 6 factors should be pursued with attention to their impact *across*, as well as within, the boundaries demarcating individual nodes (unitary or collective) within the SOS. These factors interact in diverse ways, and their interrelationships suggest a number of dimensions for research and analysis. Two examples of such interactions include:

- *Design trade-offs among comprehensivity, connectivity, and coordination.* "Comprehensivity" is the degree to which sufficient information is made available for a given actor in a given task. In a networked environment with finite bandwidth and throughput capacities (parameters of connectivity), comprehensivity can only rarely be accomplished through the trivial tactic of giving an actor all the information all the time. Even if this were feasible, it would introduce the risk of information overload. Achieving relative comprehensivity via finite connectivity for actors of finite capability requires tailoring the mass and scope of information delivered with respect to performance constraints and network capacities. This is typically handled through coordination tactics such as task specialization (division of labor), pacing, and sequencing of the information flows and displays.

- *Design trade-offs between consistency, comprehensivity, and connectivity.* Working within their specialized roles, different actors need to address an object in different ways. These differences are reflected in variations of richness and/or detail in the information sufficient for their respective tasks

(a comprehensivity issue). "Consistency" is the degree to which information affords actors mutual referentiality. There is no requirement that they address the mutually-referenced object in a literally identical manner. Effectively networking diverse actors entails a balancing act among the factors of consistency, comprehensivity, and connectivity.

Both examples are conducive to research involving information requirements analyses (IRAs) and associated task analyses. By conducting such research with respect to the SOS key intermedial factors, we can frame the research and its results in such a way as to:

(a) directly address critical performance issues
(b) relate these performance issues to informational requirements, thus informing infrastructure design
(c) relate these performance issues to task-activity requirements, thus informing operations design.

IV.B.2. Situation awareness

The most relevant current human factors / cognitive engineering area is that of *situation awareness (SA)* -- research addressing the state or character of an operator's (typically a pilot's) engagement with his/her operational environment within the context of a task. As a label for this state, "situation awareness" is typically taken to subsume the perception of momentary data, the integration of such data into coherent circumstantial comprehension, and the projection of immediate consequences for task accomplishment. SA is both the object of much constructive research and the subject of much theoretical debate (cf. Gilson, 1995). The term is used to denote two distinct things: (a) the process by which an actor acquires and maintains status orientation within a task, or (b) the state of such orientation at a given moment. By either definition, SA has the following pertinent characteristics:

- It is an informational phenomenon, and therefore an object of both offensive and defensive IW concern.
- It forms the basis for subsequent decision making and action, making it an important issue for time-critical SOS functions (e.g., TMD BMC4I).

The precise boundaries of SA are by no means fixed, and a number of definitions have been proposed. The best overview of the SA field is Vidulich *et al.* (1994),

which contains a summary analysis of this definitional morass by Dominguez (1994). The most widely-acknowledged definition of SA comes from Endsley (1988, p. 97): "...the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future." Endsley (1991) explicitly distinguishes between SA and decision making, characterizing SA as the process leading to a product (state of SA) which provides the informational basis for subsequent decision making. In the emergent approach termed *naturalistic decision making (NDM)* (Klein *et al.*, 1992 -- cf. next section), situation awareness is the core of the decision making process. Endsley's seminal formulation of SA is illustrated in Figure 6.

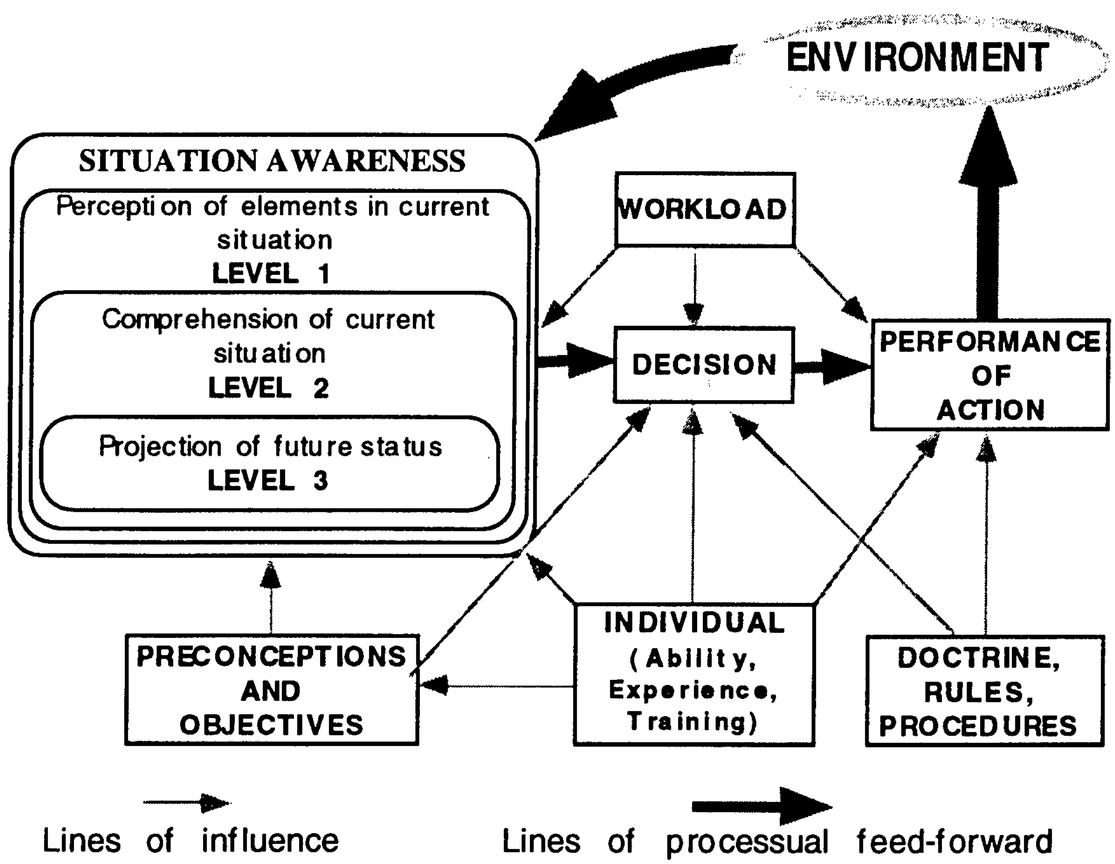

Figure 6: Endsley's Model of Situation Awareness (Adapted from Endsley, 1994)

Situation awareness (seen as either the process or the product) concerns an individual actor in the course of a task and concentrates on that actor's perception, cognition, and potential for action. Shared situation awareness (SSA) among collaborators has received less attention than individual SA (cf. Endsley, 1995;

Adams, Tenney & Pew, 1995). SSA is not simply a summation of team members' individual SA; it must be addressed in its own right. All six intermedial factors will affect the extent and quality of SSA in networked SOS, because they determine the degree to which team members can mutually and reciprocally share and manipulate the information underlying their individual and composite SA. From a cognitive engineering viewpoint, the key point of support for SSA is therefore the overlap among team members' situational information. From a systems engineering perspective, this corresponds to concerns the mechanisms by which this overlapping information is acquired, maintained, and retrieved. With respect to both viewpoints, we have delineated a specific prescription for facilitating SSA -- the *common battlespace picture (CBP)* -- as discussed later.

The primary concern of prior (individual-oriented) SA research has been the achievement of personal orientation in a task setting. SA is gauged by the effectiveness of action, but SA does not directly address action itself. As such, SA research to date is not directly informative on the means and manner in which SA feeds into decision making, or the actions executed even further "downstream." From a programmatic viewpoint, this suggests that caution must be exercised to avoid undue or counterproductive "compartmentalization" of research work and its results. The most direct solution is to integrate SA within a broader model or framework spanning the range of SOS activities. We are developing just such a framework -- the *OODA model* -- as discussed later.

IV.B.3. Decision making

Effective situation awareness is the foundation for effective decision making (Endsley, 1995). Unfortunately, SA theory to date has done little to explain the relationships between SA and decision processes. The reverse is also evident from the literature. Decision processes have to date been modeled and analyzed using finite-state quantitative classical or engineering approaches, all assuming a well-circumscribed set of issues, goals, and selection criteria as *a priori* conditions. As is the case noted for SA, such studies tend to compartmentalize their subject matter. They are mute regarding the acquisition and representational configuration of the presumed issues, goals, and criteria. Similarly, they do not typically address the "downstream" actions motivated by decisions made, or the feedback of those actions' effects into ongoing decision making.

When applied to finite and well-defined operational domains, such classical decision

models will continue to be useful. However, with respect to both military experience and emerging IW concerns, such approaches will provide progressive decreasing utility. The certainties presumed in such analyses conflict with the actual "fog of war" as confronted in modern, fast-paced military operations. IW tactics are geared to this fog of war phenomenon. They are intended to more fully "enfog" the adversary (offensive IW) while facilitating one's own clarity of SA (defensive IW). The "fog-inducing" aspects of SOS operations include:

- Ill-structured problems
- Uncertain dynamic environments
- Shifting, ill-defined, or competing goals
- Cyclical feedback on actions taken
- Time constraints and stresses
- High stakes
- Multiple actors and decision makers
- Decision criteria involving organizational goals and norms

These are precisely the factors cited by Orasanu and Connolly (1992, pp. 7, 19) in promoting a recently-emergent approach to decision making studies loosely termed *naturalistic decision making (NDM)* (Klein *et al.*, 1992). NDM has the programmatic advantage of explicitly recognizing the value of effective SA in decision making. Those formal models most representative of NDM all derive from analyses of actual decision making in action and emphasize SA (as "situation assessment" or "situation recognition") (cf. Lipshitz, 1992).

However, NDM is still best characterized as an "approach" or "orientation" rather than a rigorous theoretical or methodological framework. It provides substantial evidence on problems and general methodological corrections, but little concrete guidance on cognitive engineering issues (cf. Doherty, 1992; Klein & Woods, 1992). One avenue for constructive cognitive engineering work is to identify and configure specific cognitive engineering models and methods to the NDM-oriented aspects of SOS and IW. This would most profitably entail integrating the informational focus of IRAs with the activity-oriented perspective of task analyses. This would permit cognitive engineers to integrate decision making research within a comprehensive framework so as to avoid the sort of compartmentalization noted with respect to SA above. One such integrated framework -- the *OODA model* -- is discussed later.

IV.C. Summary: Cognitive Engineering and IW

Cognitive engineering research will most constructively contribute to USAF IW goals to the extent that (a) it focuses on IDW (as opposed to ISW) and (b) it addresses inter-actor (as well as "intra-actor") behavior and performance -- i.e., the extent to which it addresses the intermedium. This requires three adjustment relative to prior cognitive engineering work. The first adjustment is to delineate critical intermedial features or factors. The second adjustment is to review and assess situation awareness research with respect to IW needs. The third adjustment is a similar review and assessment regarding decision making research. All three adjustments constitute research innovations and constructive research results in and of themselves. These adjustments will, in turn, provide a basis for extending and refining cognitive engineering expertise in information requirements and task analyses (yet another programmatic payoff).

Cognitive engineering for information dominance should address the key operational characteristics specific to the intermedium in which IW is realized -- the six *intermedial factors*. These provide a set of testable parameters upon which research studies can be planned and conducted. This accomplishes the first methodological adjustment prescribed earlier. We have then presented and discussed the promises and pitfalls of pursuing two cognitive engineering topics -- situation awareness and decision making -- with respect to the novel aspects of distributed SOS and IW. This accomplishes the second methodological adjustment prescribed earlier. In Section V. we shall lay out the goal of such research work -- a proposed IW-oriented solution path for improving USAF theater SOS.

V. THE GOAL: A COMMON BATTLESPACE PICTURE

In this section, we shall introduce and describe our proposed class of solutions for improving networked BMC4I in a theater SOS. This proposed solution will entail technical and procedural interventions in the intermedium, optimize the intermedial factors, and improved situation awareness and decision making.

V.A. The Criticality of Shared Information Spaces

One obvious approach to optimizing networked SOS operations is unifying the pool of information upon which all actors depend and managing this pool in such a way as to effectively and efficiently deliver "the right information to the right warfighter at the right time" (Owens, 1995). Such an approach is consistent with the state of the art in both SA theorization and IT innovations supporting decision making. Endsley (1995, p. 39) specifically claims the overlap among team members' SA information bases "...constitutes much of team coordination," and she suggests "...the quality of team members' SA of shared elements (as a state of knowledge) may serve as an index of team coordination or human-machine interface effectiveness." The notion of a *shared information space* -- "...a medium that could be used dynamically ... to help people to share their view of the world with others through joint manipulation of each person's personal models of the situation" (Bannon, 1989, p. 13) has become a key concept in the field of *computer-supported cooperative work (CSCW)*, and implementation of such a common resource is the cornerstone of advanced *group decision support systems (GDSS)* (Kraemer & King, 1988).

By prioritizing equal access to critical information across the widely-distributed set of SOS actors, potential bottlenecks in current communications layouts can be minimized (i.e., better connectivity and consistency). By prioritizing sharing of critical data, potential breakdowns and disruptions in the informational feed-forward from sensors to weapons delivery can be minimized (i.e, better comprehensivity, comprehensibility). Furthermore, performance throughout the SOS will be enhanced by all actors' ability to orient themselves and their actions with respect to a common "picture" (i.e., better congruence and coordination). This will enhance overall SOS integrity. We believe this more robust alternative to current BMC4I infrastructures' "bucket brigade" mode of data feed-forward can be obtained with operational costs (e.g., messaging traffic burdens) no higher than those already implicit in projected architectures.

This approach is dependent upon the creation, maintenance, and utilization of a

shared information pool which we term a *Common Battlespace Picture (CBP).* In many respects, the line of argument in favor of a CBP mirrors the reasoning that led to the development of *database management systems (DBMS)* in the 1960's. That earlier effort was motivated by the same concerns of efficiency, effectiveness, and integrity of data / information management in large distributed organizations. In the military arena, CBPs meet the demands of high-performance, integrity-dependent, information-intensive operations of potentially global scope.

In the formulation of DBMS strategies in the 1960's, the term *database* was used in a figurative sense, connoting the collective information resources as they were available to a given user, not necessarily as they were physically stored. Because our focus is on human factors / cognitive engineering, this user-centered viewpoint is the perspective from which we work. Therefore, we use the term "common battlespace picture" to mean a fused depiction of battlefield status available to a given warfighter, without assuming it to denote a literal concentration of data at one physical site. In other words, our cognitive engineering focus prioritizes the CBP's usability for warfighters independent from its physical / technical implementation details.

V.B. Key Features of a Common Battlespace Picture

To link and coordinate a population of warfighters to achieve the objective of consistent battlespace understanding, an effective CBP should exhibit four operational characteristics, which are in turn linked to the six intermedial factors discussed above. These characteristics are:

- *Mutual accessibility.* For the CBP's information to be useful, it must be available to the "right warfighter." Whether deployed as a centralized or a distributed asset, the CBP must be accessible by all relevant actors. The particular time and space distribution of the CBP may vary, but accessibility to its pooled information may not. This characteristic will vary according to the system's degree of effective connectivity and consistency.

- *Mutual interpretability.* Actors with differing specializations often address mutual problems through differing knowledge schemas and terminology. This variability can induce a counterproductive "Tower of Babel" effect (cf. Boff, 1987) which slows or prevents information sharing. Given the short operational timeframes for modern operations (e.g., TMD), there is little

opportunity for clarification and / or translation. An effective CBP must therefore make provision for individual actors' frames of reference with respect to the information delivered to them. This characteristic will vary according to the system's degree of effective comprehensivity and comprehensibility.

- *Mutual meaningfulness.* Actors fulfilling differing roles address a mutual problem at different times and in different ways. Simple delivery of usable information (i.e., fulfilling only accessibility and interpretability) is not sufficient to guarantee its effective and efficient application in an activity. Effectiveness can be impaired by trivial or irrelevant information, and efficiency can be impaired by information overload. To promote good situation awareness in distributed teams, a CBP must provide the "right information at the right time" (when realized through individually-targeted distribution) and the "right information at all times" (when realized as a central pool). In other words, an effective CBP must make provision for individual actors' frames of reference with respect to the activity to which they are applying the information. This characteristic will vary according to the system's degree of effective congruence.

- *Mutual manipulability.* Teams must coordinate themselves, and their ability to do so will have a major effect on their composite performance. One channel for accomplishing this consists of the command and control links by which (e.g.) CRC exerts direct coordination over a TMD team. Another channel consists of the more general links by which one actor may indirectly coordinate others by updating information to which they must respond. As a common reference pool, a CBP would provide an obvious foundation for such indirect coordination. This beneficial effect requires that individual actors have the ability to manipulate (e.g., correct, update) their common information pool. This characteristic will vary according to the system's capacity for coordination.

Conclusions. Facilitating the development of functionally-integrated CBPs requires focusing on *information requirements analyses (IRAs)* of existing tasks and CBP models for purposes of evaluation, validation, performance assessment, and generation of requirements specifications.

VI. THE MEANS: THE OODA MODEL

VI.A. Introduction: The OODA Loop

The most-cited theoretical construct in the IW literature is the *OODA Loop* of Col John R. Boyd (Boyd, 1987). The number of references to Boyd's OODA Loop in the C^2 / C^3I / C^4I / IW literature is impressive; Hammond (1994) claims over 50. This has to be considered extraordinary, given that (a) the primary reference material (Boyd, 1987) consists of a set of unpublished briefing slides, and (b) there are no detailed expansions of Boyd's ideas elsewhere in the literature. There are occasional variations on the label (e.g., *O-O-D-A Loop* per Mann, 1994; *observe-orient-decide-act* sequence per Sullivan & Dubik, 1994), but the reader is not likely to see a reference to Boyd's work which is unrecognizable. For the purposes of this discussion, we will employ the simple form "OODA Loop."

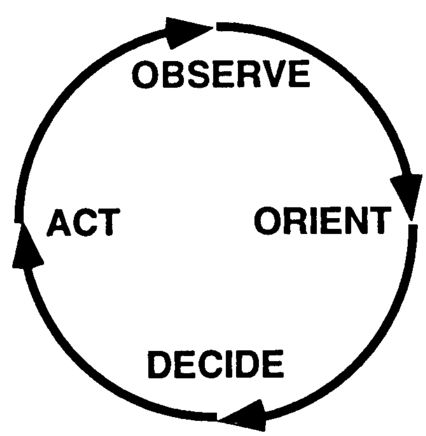

Figure 7: The OODA Loop (per Boyd, 1987)

The OODA Loop is currently taken to be a cyclical model unifying the perceptual / cognitive / enactive factors in decisionmaking. The acronym "OODA" stands for *Observation - Orientation - Decision - Action*, and the "loop" connotes a cyclic iteration through these four steps (cf. Figure 7). Related concepts found in the military literature include: *see, think, and strike loop* (Emmett, 1994); *knowledge-feedback cycle* (Jensen, 1994); *analyze, act, and assess* (Fogleman, 1995a); ; *(Stimulus-Hypothesis-Options-Response) paradigm* (Wohl, 1981; Wohl, Entin & Eterno, 1983) and *decision cycle* (Sullivan & Dubik, 1994, specifically, and many others generically). Boyd applied the concept initially to analyze individual fighter

pilots' performance in the Korean War (cf. Morton, 1995; Simpson, 1980). Boyd's (1987) written use of the concept addresses tactical command and control in military history.

In the IW literature, the OODA Loop is invoked to illustrate information dominance's practical payoff -- the ability to act (and react) in an informed, knowledgeable manner faster than the adversary. Achieving this temporal decisionmaking advantage is termed "operating within the enemy's decision cycle" or "operating within the enemy's OODA Loop." The general idea is to act (repeatedly) in such a way as to (a) provide the adversary with an apparent scenario or set of options conducive to one's own goal(s) and (b) deny the adversary sufficient time to analyze these actions and the results (apparent scenario / options) with respect to their validity.

The temporal coercion aspect is the same strategy outlined in classical analyses of propaganda: "The propagandist seldom wants careful scrutiny and criticism; his object is to bring about a specific action." (Lee & Lee, 1939, p. 13) Operating within an adversary's OODA Loop through information warfare tactics matches Lee's (1994) strategy for achieving information dominance:

> "Military actions directed against the enemy should be undertaken with the strategic objective of delaying, disrupting, and denying information used by the enemy leadership for the effective execution of military strategy. ...(T)he strategic center of gravity is the enemy leadership, both military and civilian, that rely on information to execute the national military strategy. In essence, the end game is to coerce the enemy by increasing his uncertainty regarding his ability to successfully execute his military strategy." (p. 29)

For all its deceptive simplicity, Boyd's OODA Loop incorporates several key features which make it useful as a construct in human factors IW research. First, it explicitly addresses the decision cycle in terms of continuous process from perception (Observe) through cognition (Orient / Decide) to response (Act). This maintains a scope identical to the scope of the application issue (e.g., command and control). Addressing this full application scope allows researchers to proceed without necessarily decomposing the subject process into multiple (and potentially irreconcilable) sub-models. In turn, this lessens the probability of counterproductive compartmentalization or "tunnel vision." Second, the OODA model orders the

decision / action process in such a way as to correspond to relevant analytical models such as the *abstraction hierarchies* of Rasmussen (1986). This permits systematic reciprocal translations of issues, data, and conclusions among these models and the OODA model. Third, the OODA Loop explicitly ties a system's perceptual / cognitive process to that same system's action toward its operational environment, and vice versa. This maintains focus on the given system of interest and minimizes explanatory digressions.

VI.B. The OODA Loop as a Research Model

We are developing the basic OODA Loop construct into a model for organizing human factors research in IW. This requires us to take the connotations of the OODA construct from available literature, then devise definitions and rules which formalize those connotations into a structured model. As a first step, the fundamental unit of analysis -- the OODA Loop --is defined and qualified axiomatically as follows:

- An *OODA Loop* consists of four *phases* -- *Observe, Orient, Decide*, and *Act*.
- In its canonical form, an OODA Loop is comprised of a single relative ordering of these four phases in the sequence "*Observe, Orient, Decide*, and *Act*."
- No event / behavior loop violating the O-O-D-A relative ordering (e.g., O-D-O-A) will be considered an OODA Loop.
- One or more phases may be deemed "null" or "circumvented" in describing a specific event / behavior sequence, subject to the constraint that the relative ordering is maintained (e.g., "reflex" seen as a direct transition from "Observe" to "Act").
- Event / behavior loops exhibiting the prescribed relative ordering, but delineated in something other than the canonical form (e.g., A-O-O-D Loops) are left as an open issue pending further development of the model below.

These propositions lay out the basic ground rules for OODA Loops as abstract units. The following describes the four individual phases comprising a unit OODA Loop with respect to an individual subject:

- *Observe phase.* In the Observe (Ob) phase of an OODA Loop, the subject, operating within his / her role, engages phenomena in the environment within which he / she pursues the process. Observation consists of the subject's transformation of phenomena into a set of data The Observe phase concludes at the point that the subject begins integrating this data into his / her knowledge base.

- *Orient phase.* In the Orient (Or) phase of an OODA Loop, the subject, operating within his / her role, engages data deriving from observation. Orientation consists of distilling information ("any difference that makes a difference" -- Bateson, 1987) from the data stream and integrating that information along with prior facts and understandings into a coherent state of situational knowledge. The Orient phase concludes at the point that the subject achieves this coherent state. Note that the criterion for Orient phase completion is a "coherence" of situational knowledge, not a "completeness" or "accuracy" of situational knowledge.

- *Decide phase.* In the Decide (D) phase of an OODA Loop, the subject, operating within his / her role, engages situational knowledge deriving from orientation. Decision consists of evaluating this situational knowledge, projecting its ramifications for the process, focusing on a set of chosen ramifications, and selecting action(s) appropriate to that focus (a plan). The Decide phase concludes at the point that the subject moves from reflection on to enactment of the selected action(s).

- *Act phase.* In the Act (A) phase of the OODA Loop, the subject, operating within his / her role, engages the process environment with respect to the plan deriving from decision. Action consists of transforming the abstract plan into instrumental behavior. The Act phase concludes at the point that the subject completes or interrupts realization of the plan and begins observing the newly-changed state of the process environment.

The following points are introduced to qualify the abstract OODA model in preparation for its application to actual systems:

- There is no presumption that an OODA Loop, once begun, will necessarily be completed.

• Precise delineation of transitions from one phase to the next may appear context- or situation-dependent. As such, there may be variations among mappings of specific event / behavior sequences onto the O-O-D-A phase sequence.
• No presumptions are made about the absolute or relative durations of the four phases.
• No presumptions are made about the overall composite duration of a unit OODA Loop.

VI.C. Iteration and Recursion in OODA Loops

The next step in this process is to make explicit a feature which is implicit in Boyd's (1987) original OODA delineation and subsequent literature. This feature is the innate iterative quality of the OODA Loop -- i.e., the idea that a given actor proceeds through an ongoing, repetitive series of O-O-D-A sequences, as illustrated in Figure 8. For a given subject, iteration proceeds from loop to loop via a transition from Act to Observe phases (cf. Figure 8). Unlike the informational transitions between the four phases within a unit OODA Loop, the Act-Observe transition entails an instrumental feed-forward, in which the results of the Act phase modify the subject's situation within the operational milieu and thereby affect his / her ongoing ability to Observe.

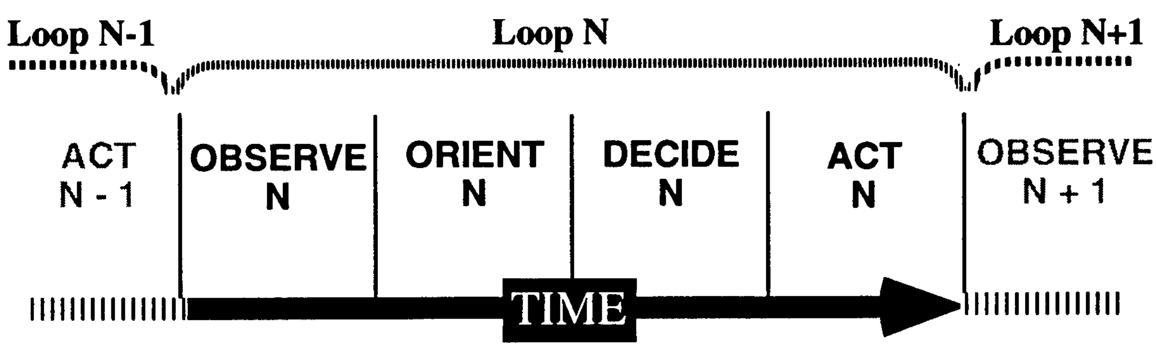

Figure 8: Continuous Iteration in the OODA Loop Model

This inherent iterative character permits the model's application to ongoing decision / action processes (as opposed to being constrained to single abstracted instances). The IW literature typically treats the OODA Loop in just this way (e.g., Widnall & Fogleman, 1995, p. 7). This iterative character can also be treated as recursive, permitting the same OODA Loop model to be applied across different levels of systems (e.g., units and their components) and processes (e.g., overall missions

and atomic tasks). The iterative / recursive nature of the OODA model allows it to address the task performance of an individual operator who accomplishes multiple subtasks, whether linearly ordered or conducted in parallel.

VI.D. Mapping OODA Loops onto Processes, Subjects, and Roles

The iterative and recursive nature of OODA Loops permits us to extend the basic OODA construct when modeling activity in systems of arbitrary extent and complexity. Formal specifications for a structured OODA depiction (termed an *OODA map*) and specific tactics for OODA modeling are being formulated by CIWAL. This work is being detailed in a separate CIWAL document entitled *The OODA Model: An application of Boyd's 'OODA Loop'.*

VI.E. How the OODA Model Fits the Needs of Cognitive Engineering for IW

The OODA model as elaborated thus far concentrates on the pattern and course of activities in an operational domain. This focus is deliberate, and we believe it fits the scope and form of the issues in IW. Generally, applying an OODA approach is justified by the following:

- *The OODA model prioritizes action over artifacts.* The OODA model is a tool for addressing SOS decision processes -- i.e., "...the planning, tasking, and control of the execution of missions through an architecture of sensors, communications, automation, and intelligence support" comprising their BMC4I (Wetzel and Kowall, 1994, p. 2) The Action-priority of the OODA model is geared toward (a) illuminating how such planning, tasking, and control functions can be effectively conducted with current infrastructures, and (b) informing how current and prospective infrastructures can facilitate these functions. In other words, the OODA model is based on the priority of the mission over the means.

- *The OODA model prioritizes practical theory over theories of practice.* There are many theoretical frameworks available for addressing perception, cognition, decision making, coordination, and operational efficiency. Most

of these are useful only to the extent that actual operations can be interpreted to fit into the perspective of a model initially crafted to be compelling to a scholarly community. The OODA model's focus corresponds to the need to be compelling to a practicing military community. The adoption of Boyd's (1987) OODA Loop represents the construction of analytical tools based on warfighters' own practical theorization.

- *The OODA model is both systematic and systemic.* Reductionist models of processes offer tools which are usefully *systematic* (organized; structured) but fall short of treating those features of complex phenomena which are *systemic* (addressable only in terms of the overall phenomenon being studied). An example would be detailed Simonian models of decision making, which take Observation and Orientation as given and leave Action outside their scope. The OODA model provides sufficient structure to be systematic, while maintaining a scope equal to the systemic nature of its target application -- SOS decision processes. This minimizes the pitfall of isolated and compartmentalized results.

- *The OODA model minimizes reliance on a particular analytical theory or model.* The OODA model's activity focus is intended to minimize commitment to, and constraint by, one or another particular model of perception, cognition, information processing, etc. This does not mean that the OODA model precludes the application of such models. In fact, the opposite is true -- the OODA model provides a grounded framework into which more specific models can be connected to address features of subject systems and their interactions.

The last item -- minimum reliance on a particular theory -- raises the question of how the OODA model relates to the variety of theories, approaches, and tools already available for human factors / cognitive engineering research. In the next section, we shall discuss the relationships between such current work and our proposed OODA model.

VI.F. How the OODA Model Relates to Current Cognitive Engineering Work

The OODA model is based on the idea of perception / decision / action cycles. In other words, its central theme has to do with an entire process of informed action. One must ask if a new OODA model is really necessary, given the variety of existing cognitive engineering tools and techniques for mapping out the form and flow of activities. We believe an OODA model complements (rather than supersedes) such other approaches by providing a framework within which their respective strengths can be better exploited.

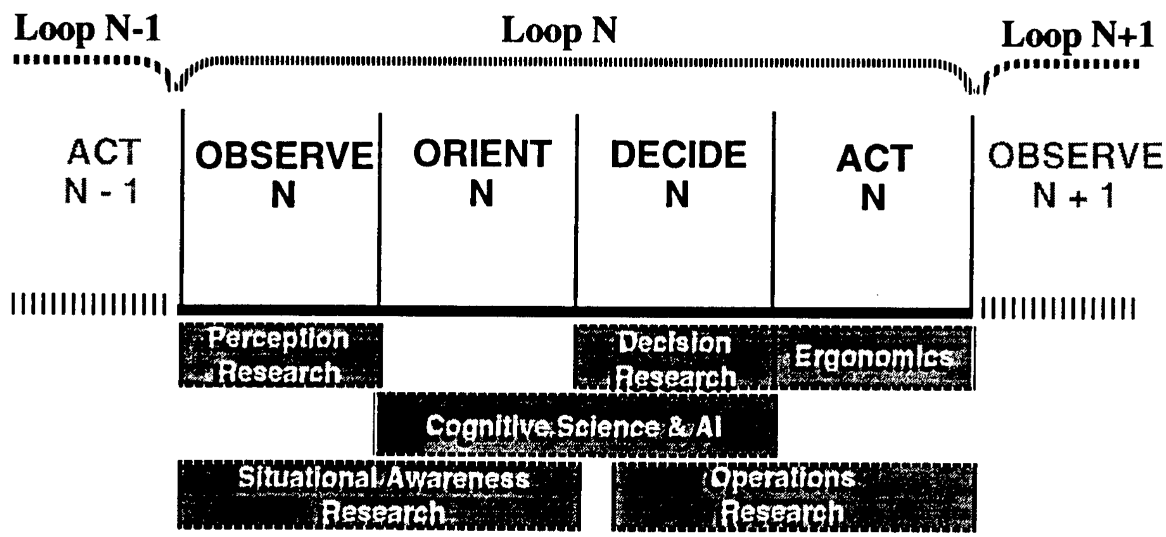

Figure 9: How Current Research Fields Address the OODA Loop

The best way to illustrate the OODA model's relationship to prior human factors work is to do just the reverse -- show the phases of the OODA Loop primarily addressed by current research specialties. This is illustrated in Figure 9. Even though each field's scope of intersection with the OODA cycle is subject to interpretation, it should be clear that not one of them addresses the entirety of the cycle. By the same token, the figure illustrates the point(s) at which theory, results, and applications from each of these research areas could be constructively applied to an OODA model for a given activity.

In the following two sections, we shall discuss the OODA model with respect to examples of such available tools and techniques, categorized into the two broad classes relevant to cognitive engineering:

(1) *Methods for analyzing information capacities.* These focus upon the generation, transfer, and application of data and information in an activity. In the realm of pure research, such work includes (e.g.) studies of perception and cognition. The realm of applied research, this focus is typical of cognitive workload analyses, decision analyses, information systems requirements analyses, and the like.

(2) *Methods for analyzing action capacities.* These focus upon the execution and coordination of task actions. In the realm of pure research, such work includes (e.g.) ergonomics, operations research and the engineering of activity system capabilities. In the realm of applied research, this focus is typical of physical workload analyses, efficiency studies, and the like.

Each of these two approaches is potentially useful. Neither, however, is guaranteed to provide results which are constructively applicable. An extreme concentration on information capacities can lead (and has led, in some cases) to highly-abstracted theorization whose primary payoff is to (e.g.) academic psychologists. An extreme concentration on action capacities can lead (and has led) to highly-structured activity models which, when realized in systems, are both limited and limiting. Our invocation of Boyd's OODA Loop is an attempt to unite these two foci (and the tools associated with them) into a more comprehensive framework for researching information-intensive mission-critical SOS architectures. We see this as a fundamental condition for handling the complexities of the necessary work.

VI.F.1. The OODA model and analysis of information capacities

The Observation phase of the OODA Loop has primarily been addressed by *perception research* (for human actors) and *sensor engineering* (for artificial systems). Work typically done under the labels of *cognitive psychology* or *cognitive science* has addressed the central Orient and Decide phases of the OODA Loop. The Decide phase is also the focus of work in a variety of specialties which we will combine under the label *decision research.* During the last 2 decades, such work has typically been framed with regard to a signal detection paradigm for perception and a computational or information processing paradigm for cognition and decision making. This perspective has prioritized issues of symbolization and

symbol manipulation over issues of Observation (i.e., perception) and Action. Generally speaking, Observation and Action have been approached only in terms of how incoming data and outgoing impulses for action (a) are coded internally and (b) exhibit coherence with an internal symbolic model.

The results of this work could usefully inform the means for structuring analyses of human operators' performance during the first three OODA phases. More specifically, this utility would be most pronounced in planning and conducting *information requirements analyses (IRA's)* for a given task. Cognitive science approaches could also be usefully applied to laying out formal and functional interrelationships among data and information units relevant to a given task (e.g., data streams, task logic, operator mental models). Because the OODA model emphasizes action in the operational environment, its application as a programmatic framework would help avoid the pitfall of concentrating solely upon abstract information models to the point that they limit, distort, or lose sight of instrumental activity.

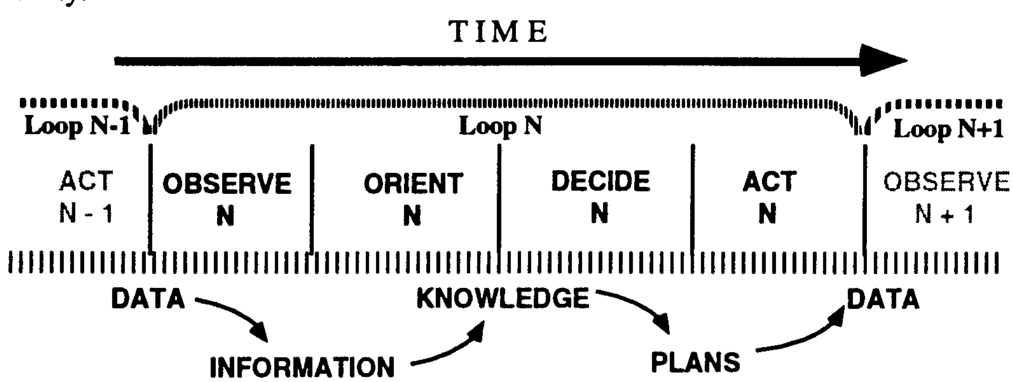

Figure 10: Information Process in the OODA Loop

This does not mean that the informational aspects of decision / action cycles can or should be ignored. To adequately analyze the intersection of instrumental and informational factors involved in information dominance, one should have the ability to account for both in whatever model(s) underlie an IRA. If one starts with the OODA model, such an accounting requires a satisfactory mapping between (a) specific types or levels of informational artifacts and (b) the activity stages of the OODA process path. A generic outline of such a mapping is given in Figure 10.

The feasibility of drawing such correspondences between informational artifacts and activity phases can be clearly demonstrated by comparing the OODA Loop with the SHOR (Stimulus-Hypothesis-Options-Response) model describing decision tasks

within command and control (Wohl, 1980; Wohl, 1981; Wohl, Entin & Eterno, 1983). Like the OODA model, the SHOR model was developed to address decision making in the military SOS, and it can be delineated graphically with respect to the entire scope addressed by the OODA Loop (cf. Waltz & Llinas, 1990, Figures 8.6 and 8.7, pp. 270-271). The primary difference between the models is that the primary dimension for delineating progress in the OODA model is activity, whereas in the SHOR model progress is structured with respect to specific classes of informational artifacts. Beyond this difference of perspective, the two models are remarkably similar in their four-part breakdowns of decision / action cycles. A summary illustration of their correspondences is given in Figure 11.

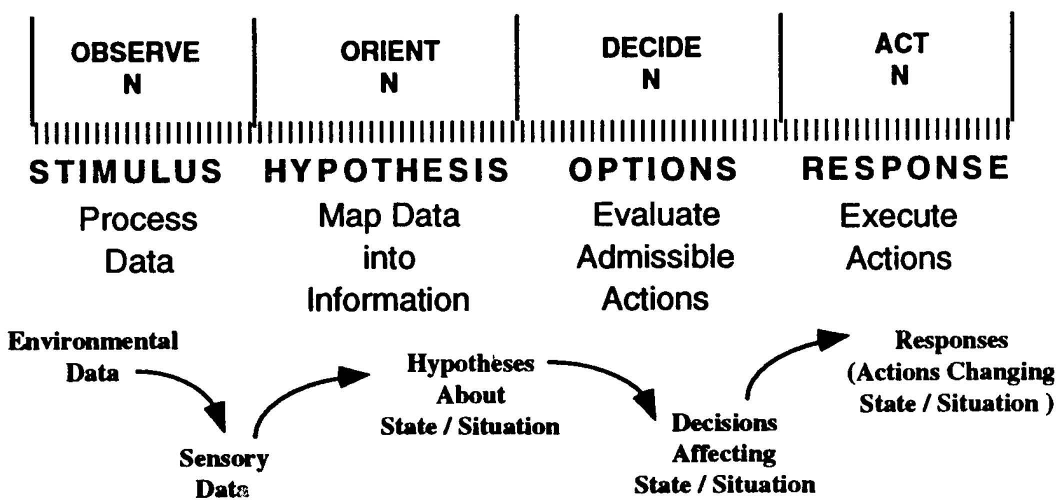

Figure 11: Correspondences between the OODA and SHOR Models (SHOR Descriptions Adapted from Wohl, Entin & Eterno, 1983)

Any comprehensive IRA (or set of IRA's) will need to span the entirety of the subject process path. Both the OODA and the SHOR models provide a basis for compiling such a comprehensive analysis by being structured with respect to a unit decision / action event. The correspondences between the OODA and SHOR models are sufficiently straightforward to provide a common frame of reference for generating either information- or activity-oriented analytical representations. This suggests that it is feasible to extend one or the other representation in accordance with these models' similarities so as to provide the bridge between the informational and instrumental aspects of decision / action cycles in the SOS. Work toward a more precise mapping between the OODA model and (e.g.) the SHOR model is ongoing.

One might well ask why we have elected to address informational factors by building upon the activity-oriented OODA model rather than by (e.g.) extending the SHOR model to explicitly address the course of activities. One reason is that the activity phases of the OODA Loop can be readily treated as recursively decomposable, while the information classes delineating the S-H-O-R subunits cannot. This gives the OODA model an advantage in that it can be 'scaled' through recursion to fit multiple levels of composite activity. An equivalent tactic for the SHOR model has not been satisfactorily defined. Another reason is that our focus on human factors and human performance is geared toward a prioritization of action. Yet another reason is that transitions among activity phases are more readily distinguished empirically than transitions among the intent or interpretation of informational artifacts.

The OODA model is the first step in our ongoing work toward generation of comprehensive IRA tactics. In the following two sections, some of the key issues in this work will be illustrated with respect to two overarching concerns in cognitive engineering -- *situation awareness* and *knowledge representation.*

VI.F.1.a. An example: The OODA model and situation awareness

Perhaps the most relevant current human factors / cognitive engineering area is that of *situation awareness (SA)* -- research addressing the state or character of an operator's (typically a pilot's) engagement with his/her operational environment within the context of a task. The key distinction between the OODA model and situation awareness research lies in their foci. The OODA Loop is a descriptive model of the event trajectory followed by an actor in accomplishing some task. It integrates those aspects of performance typically segregated on the basis of perceptual, cognitive, and/or instrumental characteristics. Situation awareness (seen as a product) is an ascribed state or quality of the actor in the course of a task, focusing on the actor's perception, cognition, and potential for action. SA is gauged by the effectiveness of action, but SA does not directly address action itself. By mapping SA onto the OODA Loop, we can achieve the necessary linkage between SA and action.

The first half of the OODA Loop (i.e., the Observer and Orient phases) closely approximates Endsley's definition of SA as "...the perception of the elements in the

environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future." (1988, p. 97) This linkage between the Observe / Orient phases and SA is straightforward and occurs in the literature (e.g., Stiffler, 1987; 1988; Llinas, 1995). The "end point" of this correspondence is made more clear by Endsley's (1991) explicit distinction between SA and decision making. She clearly characterizes SA as the process preparatory to decision making and its product (state of SA) as the informational basis for subsequent decision making.

Situation awareness sets the stage for effective decision making (cf. Endsley, 1991). An Orientation phase concludes with the attainment of the "mental picture" fed forward in the given OODA Loop in which it occurs. Future-directed aspects of that orientational state (e.g., forebodings, apparent trajectories, implications) are possible and permissible, but they are neither necessary nor sufficient. The key phrase is "fed forward," not "attainment" or "mental picture." There is no requirement that the Orientation phase persist until some optimal or full state of SA is achieved. Conversely, there is no requirement that SA be achieved within the bounds of one OODA cycle.

By applying the OODA Loop construct, we shall be able to link SA research to practical gains in battlespace decision making. Deliberative future-directed speculation or prediction based on a given orientational state lies beyond the conclusion of the Orientation phase and is most constructively ascribed to the Decision phase of the same OODA Loop or to a subsequent OODA Loop entirely. In the emergent approach termed *naturalistic decision making (NDM)* (Klein *et al.*, 1991), situation awareness is in effect the core of the decision making process. As such, the mapping of SA onto the OODA Loop is potentially sufficient to provide an analytical framework for decision analyses from an NDM perspective.

In summary, the perceptual / cognitive state termed situation awareness (SA) can be mapped onto the OODA Loop's Observation and Orientation phases. The mapping laid out in this section is consistent with the majority of the SA literature and with Boyd's OODA Loop (to the extent Boyd detailed it). The ease of fit between the OODA model and SA provides a basis for readily applying SA research and results to the RMA and IW issues targeted by this document.

VI.F.1.b. Another example: The OODA model and knowledge representation tools

A variety of strategies for capturing and modeling domain knowledge have been devised over the last 3 decades. The most formally-structured work along these lines has been in the applied computing field of *artificial intelligence (AI)*. The procedures for obtaining knowledge from informants is termed *knowledge elicitation* or *knowledge acquisition*, and the structured depictions used to model the results are termed *knowledge representations*. The OODA model specifies the general requirements for a knowledge representation whose subject matter is the form and course of activity. OODA mapping necessitates a procedure for identifying and structuring this subject matter. As such, we must address the relevant connections between available knowledge acquisition practice and the requirements of OODA mapping.

The following sections address the two primary knowledge representation issues entailed in modeling the informational and instrumental aspects of a decision / action cycle. The first issue is how to model the *static elements* in the domain of interest -- i.e., those items which are persistent within the scope of the given representation. Examples of static elements in attack operations scenarios include actors, platforms, operational units, and discrete informational artifacts (e.g., messages). The second issue is how to model the *dynamic transitions* among these static elements (or sets of said elements). Examples of dynamic transitions relevant to attack operations scenarios include flight paths, force deployments, and the progression of transformations in informational artifacts (e.g., logical inferences, updates).

VI.F.1.b.1. Representation of static elements

This section will briefly illustrate knowledge representation issues with respect to one practice with which our facility has extensive experience. *Semantic networks* are a well-known knowledge representation device consisting of nodes depicting referentially-static objects and links among these nodes representing relations among the referenced objects. The arrangement and proliferation of depicted nodes is limited only by their interconnectivity (corresponding to the denoted relations), the capacities of the representational medium (e.g., a computer screen), and the level of detail provided by the informant. The advantage of semantic networks is their

flexibility of depiction and the ease with which their form is intuitively understood. They are well-suited for representing complex expansions of relatively static knowledge from a central or focal starting point. Armstrong Laboratory's Human Engineering Division has developed tools and techniques which can be utilized as part of an OODA analysis. *Concept mapping* is a knowledge elicitation procedure involving (a) iterative open interviewing interactions with informants, (b) relative control of the interviews' course by the informants, and (c) mutual focus on an emerging knowledge representation as both the product of and referential guide for the ongoing process. The knowledge representation (*concept map*) produced is an unconstrained semantic network.

Semantic networks are problematical for depicting expansions along a linear path, expansions whose depictions exceed the capacity of the available medium, and any expansion which depicts dynamic changes over time. Finally, there is a trade-off between descriptive graphical clarity and inferential effectiveness. Phrased more simply, even the most structured semantic network representations are better pictures of the domain knowledge than they are functional models usable in formal inference. For a review of these issues by a major proponent of semantic networks in AI, see Brachman (1979; 1985). As a subset of semantic networks, concept maps are subject to the same limitations. Specifically, the relatively unstructured nature of concept mapping and the resultant maps places them at the extreme of unsuitability for formal inference.

The OODA path depictions mandated by the OODA model are not well-suited for representation via semantic networks. However, descriptions involving relatively static components or states in an OODA path could lend themselves to semantic network modeling. Examples include: (a) dependencies among actors at a given time point (i.e., a "cross section" of an OODA path depiction), (b) functional relations among actors which persist through the entire activity being modeled (e.g., command hierarchies, patterns of communicational connectivity), and (c) function relations internal to subject systems and/or their roles. Given the systematic nature of the OODA model, semantic network representations would be useful to the extent that they elicit and picture a given set of momentary interactivity relations. On the other hand, semantic networks are more likely to be useful in modeling informational objects and their interrelations at a given point in time during the course of the OODA activity path.

The above discussion of semantic networks provides but one example of the issues involved in identifying specific knowledge representation tactics for OODA modeling. Other knowledge representation devices which may prove relevant in depicting OODA cycles include frames, scripts, Petri nets, rule-based inference structures, and object-oriented activity phase descriptions.

VI.F.1.b.2. Representation of dynamic transitions

Decision / action events are by definition dynamic -- the status of, and relationships among, elements of the scenario domain will change over time. There will also be changes in status and relationship with respect to the depiction and interpretation of those elements. When we address knowledge representation with respect to dynamic transitions, we must consider both (a) those transitions descriptive of the concrete scenario itself (e.g., movements, deployments, destruction) and (b) those transitions descriptive of the working description of that scenario (e.g., changes in situational assessment, logical inferences). Generally stated, these two classes of transitions correspond to the instrumental and informational aspects which interact in the scenario.

The first class of transitions (those descriptive of the scenario) have been the focus of much work toward improving data and knowledge base fidelity with respect to real-world dynamics. The second class of transitions (those descriptive of the working descriptions) is particularly relevant to IW research and development, because it subsumes those transformations which comprise the SOS information processing functions. Owing to the concern with IW tactics such as deception, one important example of this transition class would be the real-time assessment and resolution of uncertainty in the SOS data streams -- e.g., measures of (un-)certainty associated with sensor data streams or plans for action. Specific tactics for dealing with such issues include fuzzy set theory (FST), Bayesian techniques, Dempster-Shafer approaches, formal logic, and the wide variety of heuristic inference strategies (cf. Waltz & Llinas, 1990, Chapter 12).

VI.F.2. The OODA model and analysis of action capacities

Kirwan and Ainsworth (1992) provide a compendium of tactics for *task analysis*, by which they mean "...the study of what an operator (or team of operators) is required

to do, in terms of actions and/or cognitive processes, to achieve a system goal." (p. 1) The OODA model is therefore a framework for task analysis under their definition. Because the field of task analysis encompasses so many differing approaches and purposes, we should identify the OODA model's place in the set of task analyses. Kirwan and Ainsworth (p. 6) divide the numerous task analysis techniques into five broad classes differentiated by their role:

1. *Task data collection methods* -- tools and practices for obtaining data about actual task activities.
2. *Task description methods* -- the means for organizing collected task data into structured representations.
3. *Task simulation methods* -- the means for conducting dynamic run-throughs of a structured task model.
4. *Task behavior assessment methods* -- the means for testing or checking operator actions against a standard or model for activity conduct.
5. *Task requirements evaluation methods* -- the means for validating design or procurement specifications against a formal standard or model for activity conduct.

The OODA model sets out the activity phases for which data should be collected and behavior assessments made. It does not, however, specify a canonical technique or procedures for the data collection itself. The OODA mapping technique being developed by CIWAL addresses data collection, but only in terms of specifying what is to be collected. OODA mapping, therefore, is best characterized among Kirwan and Ainsworth's *task description methods* -- "...techniques which structure the information collected into a systematic format...[which]...may then serve either as reference material to enhance the understanding of the human-system involvement, or may be used more directly." (p. 36) This definition's allusion to generation of material for subsequent use sets the stage for illustrating the OODA model's relationship to simulations, behavior assessment, and requirements evaluation. OODA maps and other results can be fed forward to provide the reference point(s) for these activities.

The OODA model does not limit the range of data collection techniques which may be employed, so long as they are employed with respect to all phases of the OODA Loop. Collation of OODA data can employ the sort of *charting and network techniques*, *operational sequence diagrams*, and *timeline analyses* listed by Kirwan

and Ainsworth. The OODA model's treatment of activity cycles as decomposable into subloops makes it compatible with other *decomposition methods* and *hierarchical task analyses*. The primary innovation of an OODA model is not so much its enforcement of specific task analysis tactics or techniques, but its requirement for conducting such analyses so as to address the entirety of the subject's activity path from Observation through to eventual Action. Another difference is that the OODA model is geared to modeling activity which is cyclically performed by a given subject. This contrasts with most task description techniques, which treat the operation as the primary subject and lay it out linearly.

In the following two sections, we shall outline the points of correspondence between an OODA Model and two specific task analysis schemata in use by the USAF -- IDEF and the Work Breakdown Structure. These examples will illustrate the potential for using these available techniques in the context of an OODA analysis.

VI.F.2.a. An example: The OODA model and the USAF's IDEF suite of tools

During the 1970's, the USAF ICAM (Integrated Computer Aided Manufacturing) project worked to increase manufacturing productivity through improved information technologies. This required better ways of modeling aerospace industry "activities" (defined as manufacturing cells or operational units). One of ICAM's products was the *IDEF (Integrated Definition for Function Modeling)* series of techniques, including:

- *IDEF0* , used to produce a "function model" -- a structured representation of functions, activities or processes.
- *IDEF1* and *IDEF1X*, used to produce an "information model" depicting the structure and semantics of information within the modeled system or subject area.
- *IDEF2*, used to produce a "dynamics model" -- a structured representation of the time-varying behavioral characteristics of the modeled system or subject area.

Currently, IDEF0 and IDEF1X techniques are widely used in the government,

industrial and commercial sectors, supporting modeling efforts for a wide range of enterprises and application domains. The USAF standards for implementing IDEF0 are contained in the document *ICAM Architecture Part II-Volume IV - Function Modeling Manual (IDEF0)* (1981), and the U.S. federal standards can be found in the Department of Commerce publication *Integration Definition For Function Modeling (IDEF0)* (1993). The analogous reference for USAF IDEF1 usage is *ICAM Architecture Part II, Volume V - Information Modeling Manual (IDEF1)* (1981).

The IDEF suite of modeling tools addresses one or another domain of analysis (i.e., "function," "information," or "dynamics") in a particular operation. IDEF analysis provides highly-structured depictions of the procedural interrelationships among unitary elements in each of these domains. These depictions are like static "snapshots" of the formal configuration of these elements in the abstract. Phrased another way, IDEF models provide the general "plan" of an operation. The OODA model differs from IDEF in taking activity or process as its focal point, and providing a framework for laying out the specific "events" of an operation. This is not to say that IDEF and OODA are in conflict. IDEF provides tools for laying out the general elements and relations within which specific events occur; OODA provides a framework for laying out how the human subset of these elements interoperate (vis a vis the relations) in a given instance. As such, IDEF models may constructively inform an OODA analysis, and an OODA analysis may constructively test formal IDEF models.

VI.F.2.b. Another example: The OODA model and MIL standard work breakdown structure

MIL-STD-881B (25 March 1993) provides a structured decomposition method for laying out and tracing the contractual work supporting DOD materiel acquisition. This decomposition is termed a *work breakdown structure (WBS).* The OODA Loop provides a basis for addressing and analyzing acquisition activities, as well as providing a similarly-decompositional method for analyzing USAF requirements in anticipation of procurement. As such, OODA analyses of (e.g.) TMD BMC4I systems can inform the procurement process with a minimum of reinterpretation, and OODA analyses may inform the planning and management of the procurement process itself. Conversely, the system breakdown given in a specific procurement

document can be employed as the default decompositional schema for application of an OODA analysis. As such, CIWAL's proposed OODA approach to IW-related research and development is capable of fitting in with USAF procurement as well as design activities.

VII. AN INTEGRATED COGNITIVE ENGINEERING PROGRAM

The previous sections have outlined the prospects for bringing cognitive engineering expertise to bear on issues of information warfare, particularly the achievement of information dominance. Cognitive engineering research toward this end will require an approach which integrates analyses of both the informational and the instrumental (i.e., action-oriented) dimensions of actual missions and tasks. Having now introduced and contextualized the OODA Model, we are in a position to delineate the course of such an integrated cognitive engineering program, as illustrated in Figure 12. This figure lays out a five-step research and analysis agenda which starts from description of a given mission and results in an integrated information / action analysis which can serve as the basis for requirements specifications for that mission's optimal common battlespace display(s). The five steps (plus their conclusion) proceed as follows:

Step 1: Mission Event Sequence (MES). In this step, a specific task or mission is mapped out with respect to its course of activities and a timeline. The MES results in a linear (possibly multi-path) charting of the activities which comprise the mission. Sources for mission information may include (e.g.) task specifications, records of past missions, simulation outputs, and interviews with task actors acting as *subject matter experts (SME's).*

Step 2: Dynamic Storyboarding. In Dynamic Storyboarding, the MES is modeled in a manipulable medium for study and analysis. The preferred medium is a computer-based simulation model. This permits the mission to be "played" and manipulated to determine its performance parameters. Dynamic Storyboarding "fleshes out" the schematic MES by linking specific objects, aspects, and phenomena to particular phases or points in the event sequence. This phase also allows us to lay out, order, and link the possible (or at least the expected) transitions along the MES paths.

Step 3: Decision Event Specification. In Decision Event Specification, the MES and Dynamic Storyboarding results are used to identify those points at which a particular actor must assess the situation and determine a course of action. With respect to the MES, these decision points constitute branching points from which different lines of

action may diverge. With respect to the dynamic storyboards, these decision points constitute transition points at which one of many subsequent subscenarios ("storyboards") becomes operant. Delineating critical decision events permits us to focus in on those points where transitions in the activity path are determined by states or transformations in the available information.

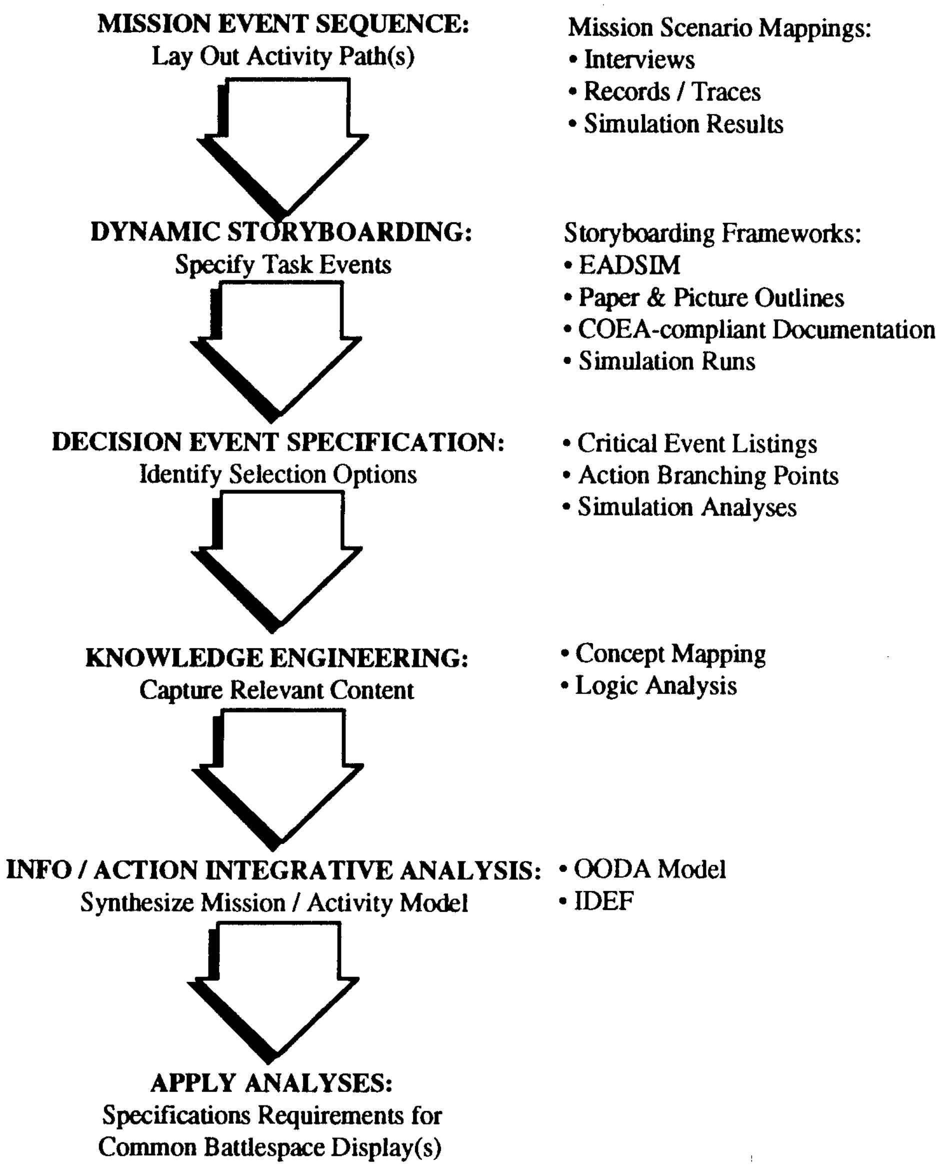

Figure 12: An Integrated Cognitive Engineering Program

Step 4: Knowledge Engineering. The critical decision events are then explored so as to lay out the data, information, and knowledge which must be brought to bear. The primary approach to this exploration is interactive knowledge elicitation conducted with mission subject matter experts (SME's). The knowledge

engineering phase results in a deeper exploration of which information parameters and what inferential strategies are important for each of the critical decision events.

Step 5: Information / Action Integrative Analysis. The MES and Dynamic Storyboarding phases have by this point laid out the activity paths for the given mission. The knowledge engineering phase (as targeted with respect to the first two phases) has provided an account of which information items, what knowledge, and which inferences are important for guiding mission / task accomplishment. At this stage, these results are brought together into an integrating framework (e.g., the OODA model) to provide a comprehensive description of the mission with respect to both its instrumental and its informational dimensions.

Application. The results of the five-step program outlined above will provide an empirical analysis from which specifications requirements can be derived or developed. Our specific orientation is to apply the instrumental / informational linkages to delineate the form, content, and accessibility profile for a literal or figurative common battlespace display supporting the given mission.

The integrated cognitive engineering program outlined above provides the means for bringing together existing practices and tools so as to comprehensively model and analyze both the instrumental and informational aspects of modern theater operations. Next (in Section VIII.) we shall illustrate the utility of this approach with a concrete example drawn from *theater missile defense (TMD)*.

VIII. A SAMPLE APPLICATION: TMD ATTACK OPERATIONS

In this section we shall step through an example scenario to illustrate some of the steps in the integrated cognitive engineering program and demonstrate their application to a specific example of current relevance -- BMC4I in theater missile defense (TMD) attack operations. Before moving to the example, we shall provide some background information on the subject area (TMD BMC4I).

VIII.A. BMC4I in Theater Missile Defense (TMD)

As a result of the Gulf War and other factors, DOD has undertaken a massive TMD effort. A key component of this initiative has been increased attention to BMC4I issues. One reason for this focus is that *theater ballistic missiles (TBMs)* afford a response window of only 5 to 8 minutes' duration, making system-of-system efficiency a critical success factor. Furthermore, TBM mobile launching systems are difficult to locate in general, and difficult to track and destroy after launching their weapons. This means that system-of-system effectiveness is also a critical success factor. Finally, there is an inherent need for better BMC4I owing to the manner in which American TMD development is being undertaken. In the near term, DOD initiatives are working toward assembling a credible TMD system out of available parts, many of which have not been associated with, much less integrated with, the command and control structure responsible for theater air defense (i.e., USAF). The increasingly large and complex set of players being assembled for near term TMD will require efficient and effective coordination to accomplish its mission.

VIII.B. Planned BMC4I Architectures for Theater Missile Defense

Figure 13 is a simplified schematic for the TMD attack operations BMC4I architecture planned for 1998 (as funded). It is representative of the range of participating units and the communication links among them. The only links shown are those between whole units. This means that any additional infrastructure for communications within units (e.g., within CRC or on board AWACS) is not illustrated. The communication links are differentiated according to general communications, sensor / intelligence data links, and channels for command and control. These links represent functional connections among the units for the

purposes noted. They do not represent a detailed or comprehensive map of the specific channels through which these functional connections are realized.

As such, the number of functional connections shown in Figure 13 must be considered either a minimal estimation or even an underestimation of the actual channels employed. In other words, Figure 13 is a conservative depiction of the communications network complexity entailed in this BMC4I architecture.

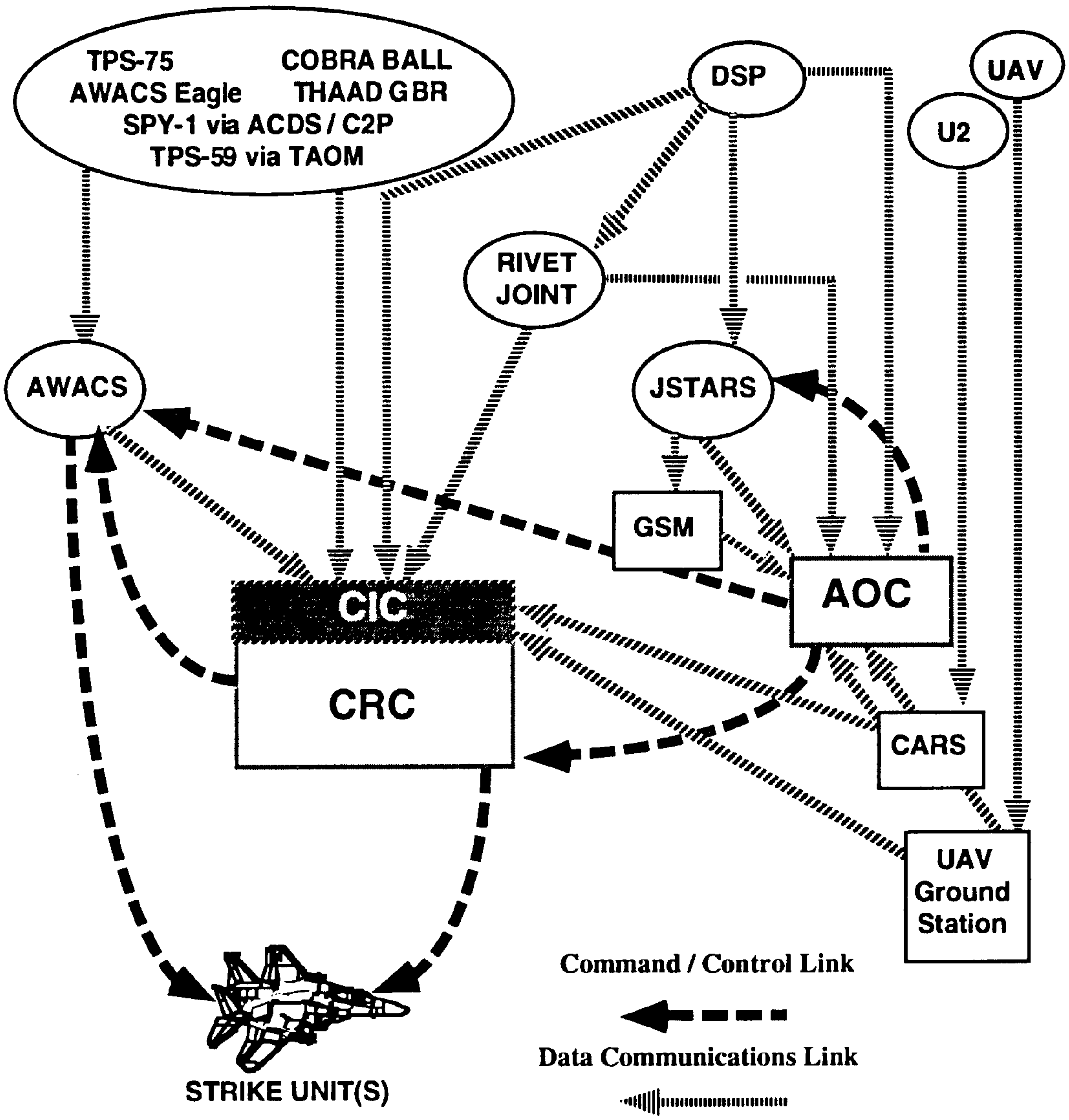

Figure 13: TMD BMC4I Architecture (1998 as funded)

	1996	1998	2002
PARTICIPATING UNITS			
	• AOC • AWACS • CARS • Cobra Ball • CRC • DSP • F15E • F16 • JSTARS • Rivet Joint • TES • TPS 75 • U2 • UAV • UAV Ground Station	**ADD:** • AWACS Eagle • SPY-1 • THAAD GBR • TPS 59	**ADD:** • *GEO satellite (1)* • *HEO satellite (2)*
TOTAL UNITS	15	19	*22*
MINIMUM COMMUNICATION LINKS [1]			
		• 4 links for 1996 units • Rivet Joint --> JSTARS • TES --> JSTARS • JSTARS/MTI --> AOC	• 4 links for 1996 units • Rivet Joint --> AWACS • All launch point detection units --> JSTARS, AOC, and Rivet Joint
AS FUNDED	29	36	61
		• *JSTARS/SAR --> AOC* • *New 1998 units --> Rivet Joint* • *TES --> Rivet Joint*	• *Downlinks for (3) satellites*
COULD BE		*42*	*64*

[1] *Link = (1) channel between two unit types* ■ = "As Funded" ■ = *"Could Be"*

Figure 14: Progression in BMC4I Architectures: 1996 through 2002

Source: Attack Operations Analysis: BMC4I Architectures, Status Review of 18 May 1995

Figure 14 provides an overview of the progression from the 1996 to the 2002 BMC4I architectures. Both the "as funded" and "could be" versions of the architectures are outlined. For each of three deployment stages (1996, 1998, and 2002), summary figures are given for: (a) the number of unit types incorporated in the BMC4I architecture and (b) the minimum number of corresponding communicational links. The set of participating units is defined and enumerated in accordance with the presumptions underlying Figure 13. The number of links is minimal, because it is based upon simplifying presumptions such as:

- one link per pair of communicating unit types
- one-way communication per link
- one channel per link
- one unit per each unit class included in the given BMC4I architecture
- adherence to the "as funded" architectures rather than the "could be" architectures (each of which entails 5 - 16% more links -- cf. Figure 14).

The set of participating unit types grows from 15 to 19 from 1996 to 1998. The 2002 "as funded" BMC4I architecture adds no new participating unit types to the 1998 version. The main innovations in the planned 1998 and 2002 architectures are the links connecting these units. The 1998 architecture adds links for the new units, plus links to feed: (a) Rivet Joint data to JSTARS, (b) TES data to JSTARS, and (c) JSTARS MTI data to AOC. The 2002 architecture adds to (a) feed Rivet Joint data forward to AWACS and (b) provides feeds for all launch point detection units to JSTARS, AOC, and Rivet Joint. Like Figure 13, Figure 14 provides a conservative appraisal of prospective TMD BMC4I.

Figure 15 summarizes the growth in complexity for prospective TMD BMC4I "as funded" architectures. Summary figures are given in accordance with the presumptions underlying figures 13 and 14. Figure 15, like Figure 13, is therefore conservative in the sense that it minimally estimates (or even underestimates) the total network complexity of each subject BMC4I architecture in its final deployed form. Even with this admittedly simplistic and conservative enumeration, Figure 15 demonstrates a rate of growth in communicational interconnectivity four times that of the population of participating unit types.

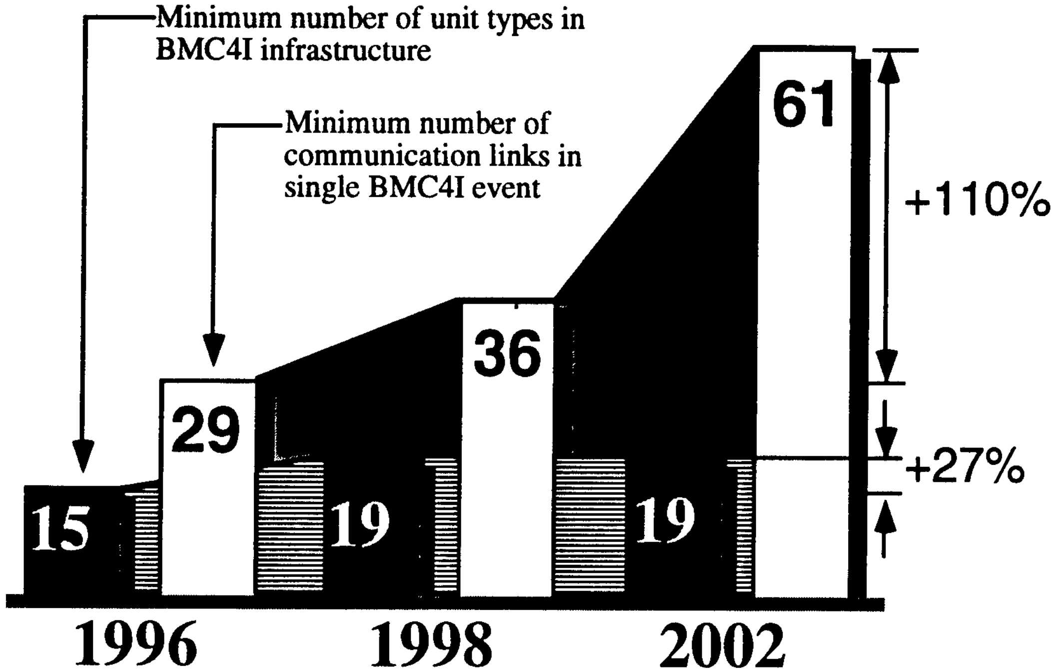

Figure 15: Growth in TMD BMC4I Complexity, 1996 - 2002
Source: Attack Operations Analysis: BMC4I Architectures, Status Review of 18 May 1995

It should be apparent from Figure 13 that each prospective TMD BMC4I architecture relies very heavily on a high-performance distributed communications network linking together all the operational TMD units. Efficient response to a theater missile threat requires feed-forward of information along the path from launch detection to battle damage assessment. Effective response requires interconnectivity among participating units sufficient to support coordination. It should be further apparent from Figure 14 that this reliance will increase with each generation of the deployed architecture. Each unit added to the composite TMD force will require one or more links to tie it into the overall TMD infrastructure. The utility of some units (e.g., reconnaissance satellites) is entirely dependent on a capacity for data communications. Figure 15's depiction of network growth outpacing unit proliferation suggests that the network is in fact the skeleton for TMD BMC4I and the critical success factor in implementing USAF plans in this area. The next section will shift to a practical illustration of these points using a concrete example.

IX. A SAMPLE MISSION: SCUD-HUNTING

Let us illustrate the growing complexities of TMD attack operations with a simplified SCUD-hunting scenario. Figure 16 outlines the major activities entailed in identifying and responding to a ballistic missile attack launched from a mobile transporter / erector / launcher (TEL). The TEL launches its missile and then flees the launch site. The TBM defensive system must detect the launch, identify the launch point, locate and track the TEL, task a response, and execute an attack on the fleeing target. This is illustrated with respect to a simplified set of TPS-75 and DSP sensor platforms, a JSTARS airborne ground surveillance platform, a CRC, and an F15E attack platform. Because the illustrated scenario is based on an immediate response, it will be termed the *immediate kill scenario*. Another likely scenario -- locating the TEL then tracking it back to its hide site before attacking -- follows the same general form, with the tasking of the F15E being delayed until the TEL is parked. This variation will be termed the *wait and pounce scenario*.

IX.A. Mission Event Sequence for the Example Scenario

The TBM response requires the coordinated efforts of all five players, which are located in different places. The first step in our integrated cognitive engineering program is to generate a *mission event sequence (MES)* for the given scenario. A composite MES is illustrated in Figure 16. The five TMD units are primarily observing data streams (DSP,TPS-75, and JSTARS) or attacking the TEL (F15E). With regard to each other, the TBM units are sending information back and forth as needed (e.g., data, commands, and acknowledgements). The only unit directly engaging the enemy (the F15E) is engaged only to the extent it receives information forwarded from other units (e.g., orders, navigational data). In turn, the units tasking and guiding the F15E (CRC and JSTARS) are themselves dependent on earlier information transfers from other units to initiate the response.

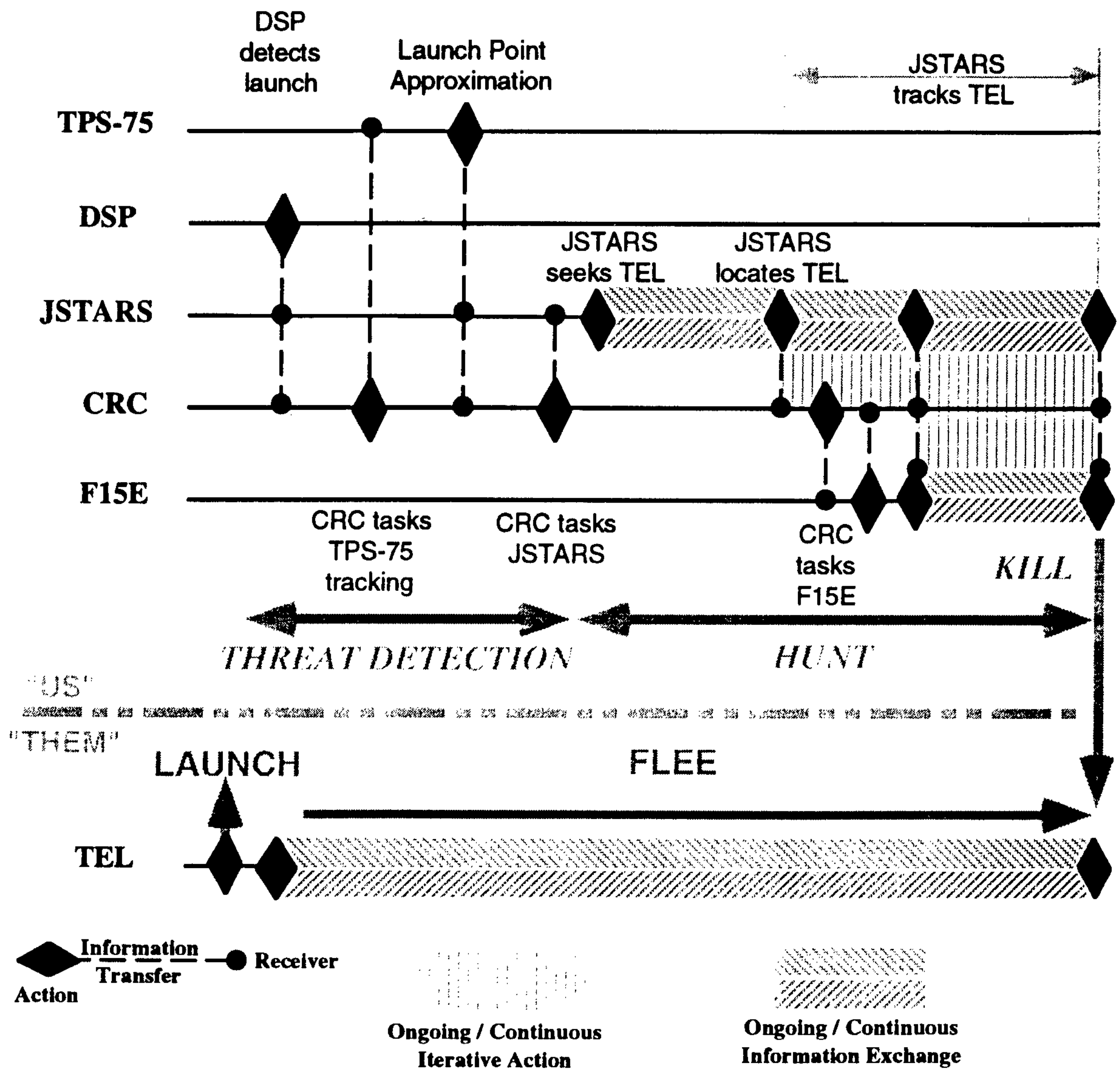

Figure 16: Composite Mission Event Sequence for a TEL Hunt / Kill Scenario

This results in a disparity between the operational needs of the TEL and those of the TBM defense system. The TEL can "succeed" during the course of Figure 16's timeline through movement and sustained avoidance of interdiction. In other words, the TEL is necessarily reliant on no more than mechanics and tactics. Similar "success" for the TBM defense system ends with the F15E's interception movements and effective execution of interdiction. This in turn must be based on surveillance, threat detection, target location, target tracking, target interception, and attack -- all tied together through CRC's command coordination. Phrased another way, the TBM system is necessarily reliant on considerably more than mechanics

and tactics. Above and beyond these factors, the defenders must depend upon (e.g.) sensor sensitivity, sensor accuracy, data processing, disambiguation skills, communications connectivity, communications bandwidth, network integrity, task allocation, resource allocation, and command decision making.

These additional "skills" all concern information -- its acquisition, its processing, and its transfer among TMD players. The TMD SOS effectiveness and efficiency are as much a result of its internal informational capabilities as its external weapons capacities. The next step is to elaborate the MES framework through Dynamic Storyboarding to discern the information flows and interrelationships which explain the activities outlined in the MES.

IX.B. Dynamic Storyboarding of the Example Scenario Using EADSIM

Dynamic Storyboarding consists of developing a scenario model reflecting the MES data and manipulating it with respect to performance parameters of interest. For the purposes of this example, our Dynamic Storyboarding was accomplished using the *EADSIM (Extended Air Defense Simulation)* software from the U.S. Army Space and Strategic Command's Testbed Product Office. This package embodies an analytical model of air and missile warfare. Using EADSIM, one can model air defense, offensive air, and attack operations scenarios for dynamic simulation and analysis. EADSIM's extensive tool set permits detailed modeling of aircraft, missiles, sensors, satellites, noncombatants, electronic warfare units, communications networks, and command and control activities. These basic players can be flexibly configured with respect to parameters such as: deployment, weaponry, sensor effectiveness, terrain, strategic areas of interest, and diverse mission types.

CIWAL has employed the EADSIM software package to lay out, execute, and analyze a variety of TMD simulations, including the simplified Scud-hunting scenario described above. Our EADSIM analysis of the two (*wait and pounce*; *immediate kill*) illustrative scenarios focused on communications coordination in the scenario's simplified SOS. Drawing on the MES shown in Figure 16, we generated a simulation involving:

- An adversary's mobile transporter / erector / launcher (TEL)
- One JSTARS airborne ground surveillance platform

- One ground station module (GSM) downloading and forwarding the JSTARS data feed
- One CRC command and control center directing attack operations
- One F15E strike aircraft

The scenario was overlaid upon a geographical data base depicting a mountainous East Asian area. The scenario's basic "plot" goes as follows. The JSTARS is patrolling in the air, the GSM is relaying JSTARS data through to the CRC, which is monitoring the air space. The F15E is flying combat air patrol (CAP). The TEL launches its missile toward a target within our protected space. Upon launch detection, the JSTARS begins searching for the launch site and the TEL. The TEL leaves the launch site as quickly as possible (some 6 minutes after launch) and retreats to a reload site. Once JSTARS has determined the TEL's location, its track, and the position of the reload site, CRC tasks the F15E to engage the TEL upon its arrival at the reload site.

Our configuration of the EADSIM models used in these simulation runs was very "conservative" in terms of situational variables and complexities. In other words, we were analyzing a "better (if not best) case" situation. This claim is based on the following points:

- Because the DSP and TPS-75 units operate as passive sensor platforms, we did not model them in our EADSIM runs.
- Only a single threat (one TEL; one Scud) was modeled.
- Only a single representative of each class of units (in a minimal set of TMD actors) was modeled.
- No AWACS platform was included in the model, so as to keep the command and control complexity to a minimum.
- Only one strike aircraft was modeled, so as to minimize the task allocation complexity.
- Sensor scanning / update frequencies were left at EADSIM's mid-range default values.
- The inter-unit messaging update frequencies were set at mid-range values (JSTARS to GSM / GSM to CRC at 72 second intervals; CRC to F15E at 120 second intervals).
- Although the models were configured over a background digital map of mountainous East Asian terrain, the simulations were modified to give the effect of an unobstructed plain (literally a "level playing field").

- Accordingly, sensor propagation variation and sensor tracking losses were filtered out of the models' execution runs.
- Similarly, message propagation variation and message losses were filtered out of the models' execution runs.

The simulations were run, and the standard statistics reports on messaging, engagement, and detection parameters were generated. For the purposes of this illustration, the most relevant result is the messaging data. EADSIM's built-in default model for interunit messaging yields a network architecture as illustrated in Figure 17. All four units generate messages, and two units (the JSTARS GSM and the F15E) feed back acknowledgement of messages received. The parameters x, y, z, and w represent the number of messages fed forward along the links they designate. The parameters x' and z' represent the number of acknowledgements (of messages in x and z, respectively) fed back to the sender along the links they designate.

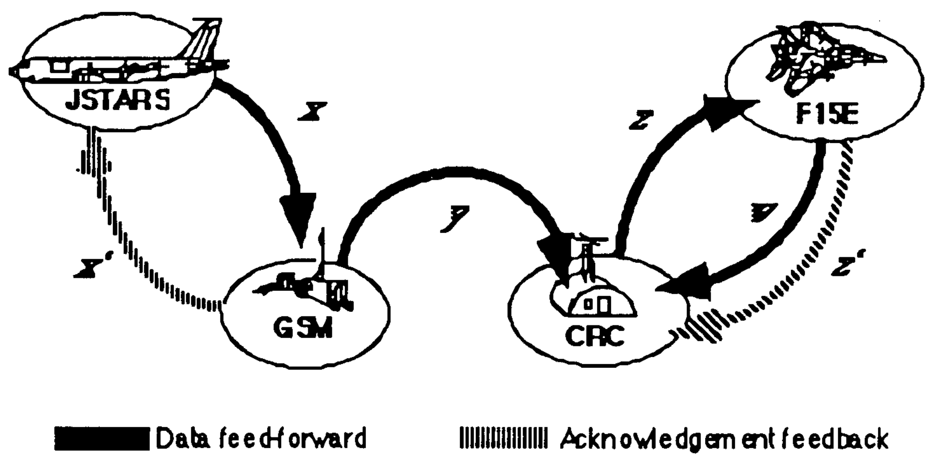

Figure 17: EADSIM's Default Networking Architecture for the Scenarios

This network architecture was tested in simulation runs of both the "immediate kill" and the "wait and pounce" scenarios. The EADSIM communications statistics are summarized in Table 1. At first glance the "wait and pounce" scenario would appear to be more "communications-intensive," because it exhibited a 53% increase in overall number of messages compared with "immediate kill." Such a view is misleading, because this greater overall traffic was spread out over a timeframe which was 85% longer. Furthermore, the majority of the elapsed time in the "wait and pounce" scenario involves TEL tracking (by JSTARS) and track reporting between the largest composite units (JSTARS and CRC). As such, the number of messages (taken in isolation) is not very informative in identifying points of possible

overload in messaging or message processing. A better metric for overall load comparison is "message traffic rate," which we computed as the average number of messages in transmission per second. With respect to both message generation and reception, the "immediate kill" scenario exhibited a 20.73% higher message traffic rate than the "wait and pounce" scenario. In other words, the overall TMD BMC4I system was more reliant on messaging effectiveness and efficiency where the style of response was driven by time criteria (i.e., swiftness of reaction).

Table 1: Scenario Messaging (Default Architecture)

EADSIM Default Network Architecture (Partial Acknowledgement)

	Wait & Pounce	Immediate Kill	Wait & Pounce	Immediate Kill
	MESSAGES GENERATED		MESSAGES RECEIVED	
JSTARS	35	18	35	18
GSM	70	36	35	18
CRC	2	11	58	38
F15E	23	20	2	11
Total messages:	130	85	130	85
Scenario length (secs):	2814	1524	2814	1524
Average messages/sec	0.046198	0.055774	0.046198	0.055774
Percentage difference in message traffic rates between scenarios:	-17.17 %	+20.73 %	-17.17 %	+20.73 %

Perhaps more significant is the fact that the "immediate kill" scenario's 20.73% increase in message traffic rate was not uniformly distributed among the TMD "players." The burden of this increase falls disproportionately upon the "downstream" half of the attack operations BMC4I chain -- the CRC and the F15E. Message traffic rate decreases by 5.04% for both JSTARS and GSM, and it increases 50.79% and 130.05% for CRC and the F15E (respectively). The total

number of messages processed (i.e., generated or received) actually declines by 48.57% for JSTARS, 48.57% for GSM, and 18.33% for the CRC. The total number of messages processed by the F15E increases by 24%. Even more specifically, the number of messages on the command link from CRC to the F15E is 5.5 times as great, and the message traffic rate 10.16 times as much, as in the "wait and pounce" scenario.

These simulation results demonstrate that the pursuit of faster response in current and prospective TMD BMC4I entails increased amounts and frequency of messages in the TMD network(s). Correspondingly, this implies that exploiting opportunities for (our) enhancing or (the adversary's) degrading our TMD abilities will increasingly involve issues of information and information networks. Effective TMD is largely dependent (and efficient TMD wholly dependent) on the informational infrastructure for BMC4I. Theater Missile Defense's reliance on efficient and effective information processing in large-scale distributed networks makes recently emergent issues, opportunities, and risks of information warfare critically important to USAF planning and implementation of BMC4I for TMD.

Clearly, it is the BMC4I infrastructure -- especially the data / communications network -- that ties together Admiral Owens' "SOS" in theater battle management generally and TMD in particular. Owens' vision of information dominance is predicated upon a commerce in data -- from its point of initial acquisition to its point of final employment -- which is both efficient and effective. For current and prospective TMD BMC4I architectures to achieve information dominance, they will have to pursue both these goals of efficiency and effectiveness. Unfortunately, the maximization of one (past a certain point) will adversely affect the other, and vice versa. This means that devising better TMD BMC4I systems will entail consideration of the relevant efficiency / effectiveness *design trade-offs* (cf. Boff, 1987) in distributed data communications. CIWAL has been extending its TMD simulation analyses toward consideration of such trade-offs by exploring points of human factors / cognitive engineering concern (e.g., cognitive burden; situation awareness) with a focus on "efficiency" as system throughput and "effectiveness" as system integrity supporting defensive IW. The remainder of this section will provide an example of this work.

IX.C. Decision Event Specification for the Example Scenario

Decision Event Specification can follow once the mission has been modeled via Dynamic Storyboarding. The following tables summarize the course of the Scud-

hunting *wait and pounce* scenario as modeled within EADSIM. The data is taken directly from an EADSIM printout, abbreviated, and "cleaned up" somewhat for understandability. Each table lists a series of event times, acting platforms (units), actions taken, and platforms (units) acted upon. The time points are given in seconds past the simulation initiation. Table 2 summarizes the activity up until the point the command center has ascertained the TEL's reload site destination and has tasked the F15E to kill the TEL. Table 3 summarizes the F15E's attack on the TEL at the reload site.

Table 2: EADSIM Trace of the Scud-Hunting Simulation (Pre-Tasking)

Time (secs.)	Acting Platform	Action	Against Platform
0.00	JSTARS		Activated
0.00	CRC	Activated	
0.00	GSM (JSTARS)	Activated	
0.00	F15E-4	Activated	
0.00	Target (Our side)	Activated	
0.00	TEL	Activated	
0.00	RELOAD SITE-1	Activated	
0.00	TEL	Missile Launch	
0.00	SCUD	Launch	
300.00	TEL	Start Up	
300.00	TEL	Launch Site Departure	
512.00	SCUD	Arrive	Target (Our side)
1137.89	CRC	Scan/Track Monitoring	Reload Site
1139.89	CRC	Scan/Track Monitoring	TEL

As can be readily seen in Table 2, this particular mission entails relatively automatic processes up to the point of task allocation decision making. The JSTARS and CRC units are occupied with acknowledging the missile launch and tracking down (via scanning) the launch site, the fleeing TEL, and the reload site to which the TEL is retreating. The decision making is limited to acknowledging the missile threat and making adjustments in sensor tactics to locate and track the aggressor.

Table 3: EADSIM Trace of the Scud-Hunting Simulation (Post-Tasking)

Time (secs.)	Acting Platform	Action	Against Platform
1190.02	F15E-4	Tasked to Attack	TEL
1190.02	F15E-4	Vectored to	TEL
1192.00	F15E-4	Approach	TEL
1329.00	TEL	Arrive at Reload Site	
1335.00	JSTARS	Scan/Track Monitoring	TEL
2812.00	F15E-4	Engage	
2813.00	F15E-4	Lock onto Target	TEL
2814.00	F15E-4	Launch Weapon(s)	TEL
2863.00	TEL	Killed by	F15E-4
2863.00	F15E-4	Determine Kill	TEL
2863.00	F15E-4	Intercept & Kill	TEL
2871.00	JSTARS	Lose TEL Track	TEL
2982.00	CRC	Drop TEL from Target Queue	Reload Site

Owing to the relatively straightforward nature of the modeled tasks and the automated character of the EADSIM simulation runs, there are few discernible decision points. The primary decisions concern target ID, location, and track projections (JSTARS), tactics (i.e., an immediate vs. delayed strike decision by CRC), and the F15E pilot's situational decision making en route and during the actual strike against the TEL. Such a lack of discernible decision points is a result of the automated simulation used here. Real world scenarios exhibit considerably more numerous and more complex decision making problems. To give an illustration, Table 4 lists the issues and questions faced by a single decision making unit (a JSTARS) where enemy TEL's are detected moving into possibly threatening positions.

Table 4: Issues for Decision Makers in Threat Detection

SITUATIONAL DECISION FACTORS IN ATTACK OPERATIONS Example: JSTARS detects vehicles moving into missile operating area ("A")	
Issues Relevant to Decision	**Potential Information Sources**
Who is in charge of area A?	• Commander's guidance • ATO (Air Tasking Order)
Where is area A in relation to the Fire Support Coordination Line (FSCL)?	• Commander's guidance • ATO (Air Tasking Order)
Who's responsible to attack this target?	• Commander's guidance • ATO (Air Tasking Order)
Who has authority to attack this target?	• Commander's guidance • ATO (Air Tasking Order)
What are the characteristics of a missile threat (e.g., form of a TEL convoy)?	• Intelligence Preparation of the Battlefield • Current intelligence
What are the emission characteristics of the possible target?	Rivet Joint, Guardrail, Compass Call, AWACS
What are the possibilities for more detailed data on the possible threat?	U2 / CARS, ATARS, visual / armed reconnaissance
What route is the track on?	JSTARS
Are there potential launch sites along the route the track is on?	• IPB • Current intelligence
Does the track match current missile activity patterns?	• IPB • Current intelligence • CTAPS-Intelligence Correlation Module
How much time is there in which to attack the target before it can launch a missile?	• Current intelligence • IPB • CTAPS-Intelligence Correlation Module
Are attack assets available?	• ATO (Air Tasking Order) • ABCCC (Airborne C2 Center) • ACE (Airborne Command Element) • AOC
Can another service attack the target?	• BCE (Battlefield Coordination Element) • CTAPS-JDSS (JFACC Decision Support System)
What effect will diverting a mission to this target have?	CTAPS-FLEX (Force Level Execution system)

Source: ACC/DRT, *Theater Missile Defense BMC4I Concept*, 10 February 1994

Table 4 provides a summary of questions which arise for attack operations commanders in response to detection of a potential threat. These do not cover the entire range of the command decision making process; they only concern the identification of the potential threat and the consideration of what options are available. Potentially relevant information sources are listed for each of the questions. The table illustrates the number and complexity of the decision issues confronting even one of the many units comprising the TMD BMC4I SOS.

IX.D. Knowledge Engineering for the Example Scenario

Owing to the automated nature of the EADSIM simulation runs, the knowledge engineering phase of the integrated cognitive engineering program was omitted from this example. The "inferential processes" relevant to the simulated activities were "hard-wired" into the simulation software's knowledge base, and were opaque to analysis or modification. Had we been analyzing a real world mission (as opposed to using the simulation), we would have explored documentation, execution records, and / or subject matter experts' contributions to ascertain the information relevant to the task and the inferential interdependencies among data and information elements.

IX.E. Information / Action Integrative Analysis of the Example Scenario

At this point we shall use the Scud-hunting example to illustrate how the OODA model can be applied to unify analyses of both a mission's informational and instrumental aspects. Table 5 (on the next page) illustrates the Scud-hunting activity outline of Figure 16, reinterpreted with respect to the OODA Loops that must be executed by the F15E pilot. The pilot's participation in the scenario is subdivided into 6 subscenarios:

1. *Fly Combat Air Patrol (CAP)* -- the activity of maintaining station pending tasking orders
2. *Receive Tasking* -- i.e., the activity of receiving, acknowledging, assessing, and responding to a tasking order
3. *Approach Target* -- the activity of vectoring toward the last / best-known location for the TEL (as provided by other actors on the TMD team -- e.g., JSTARS via the CRC)
4. *Acquire Target* -- the activity of identifying and locking onto the TEL with

the aircraft's onboard sensors

5. *Attack Target* -- the activity of bringing weapons to bear and firing on the TEL
6. *Battle Damage Assessment (BDA)* -- the activity of observing, evaluating, and reporting the results of the attack on the TEL

Table 5: OODA Phase Analysis of F15E Crew in TMD Attack Operations against a TEL

OBSERVE	ORIENT (to...)	DECIDE	ACT
	FLY CAP		
• CAP path • Instruments • Threat cues	• CAP plan • Platform status • Terrain	• Adherence to CAP plan	• Adjust flight path
	RECEIVE TASKING		
• CRC message(s)	• Tasking order(s) • Platform status	• Availability • Acceptance (of task)	• Acknowledge order • Adjust flight path
	APPROACH TARGET		
• TEL track data • Radar / Sensors • Threat cues	• Flight path • Threat • TEL path	• Best vector	• Adjust flight path
	ACQUIRE TARGET		
• Target area • Sensor data • Threat cues	• Target location • Threat	• Target ID • Target status • Target vulnerability • Weapons readiness	• Scan for TEL • Lock onto target • Select weapon(s)
	ATTACK TARGET		
• Target data • Weapons controls • Threat cues	• Rules of engagement • Weapons status • Threat	• Attack vector • Manner of attack • Weapons application	• Make final approach • Fire weapon(s)
	BATTLE DAMAGE ASSESSMENT		
• Target area • Target • Threat cues	• Evident damage • Threat	• Degree of damage • Need for re-attack • Need for egress	• Assess damage • Report damage assessment • Re-attack / Egress

For each of these subscenario sequences, Table 5 categorizes the pilot's activities with respect to the Observer, Orient, Decide, and Act phases of the OODA Loop

model. For illustrative simplicity, each of the subscenarios is treated as if it comprised one OODA Loop. Any of the subscenarios may be decomposed into more detailed OODA Loop sequences of arbitrary length -- particularly in modeling the ongoing iterations implicit in the Fly CAP and Approach Target subscenarios. At each subscenario / OODA phase intersection, Table 5 summarizes the major elements necessary to accomplish the given OODA phase within the given subscenario -- incoming data for Observation; reference information for Orient; issues for Decision; and responses for Action. This simple example illustrates the utility of the OODA model in laying out information requirements in a structured manner which can be readily related to the instrumental actions of concern.

IX.F. An Application: Communications Integrity as Defensive IW

The five-step integrated cognitive engineering program outlined above is intended to provide the basis for subsequent innovations improving the subject SOS performance. For the purposes of this illustrative exercise, we shall apply the models and results generated in the MES and Dynamic Storyboarding phases above to test the prospects for more tightly integrating the overall TMD BMC4I communications network. Phrased another way, we shall explore one simple means for modifying the current communications architecture to achieve more of a (logical; figurative) common battlespace picture shared among the Scud-hunting players.

As illustrated much earlier in this report, EADSIM's default networking architecture provides only partial acknowledgement of messages among the BMC4I players. This arrangement allows for informational integrity at the front end (the sensor downlink) and the back end (CRC control over the strike aircraft). The central link by which the GSM feeds tracking data to the CRC is one-way and unacknowledged. This affords a vulnerability in communications between the sensor and command / control units. If GSM's link to CRC is broken, there's no direct way for GSM to be made aware of it. Furthermore, corruption or "spoofing" of data passed through the GSM-to-CRC link could go unnoticed and / or uncorrected. Similarly, the link from the F15E to CRC is one-way and unacknowledged. If this link is broken, the strike aircraft's pilot has no direct way of knowing CRC is blind to his transmissions. Furthermore, corruption or "spoofing" of messages passed through the F15E-to-CRC link could go unnoticed.

Phrased another way, the most informationally-vulnerable unit in EADSIM's default network architecture is the one most central to effective TMD -- the CRC. This is an

issue of concern in assessing the defensive IW aspects of current TMD BMC4I. One way to overcome these IW vulnerabilities would be to institute and enforce full acknowledgement feedback among all TMD "players." In other words, any incoming message would trigger a (possibly automated) acknowledgement back to the sender. Such a scheme would provide the sender with immediate feedback that his / her message was received, and this would correspondingly enhance each sender's "situation awareness" with regard to downstream communications. CIWAL modified the default EADSIM message routing to reflect such full acknowledgement feedback for the two example scenarios (*wait and pounce*, *immediate kill*) discussed earlier. The resulting architecture is illustrated in Figure 18 (a modification of Figure 17).

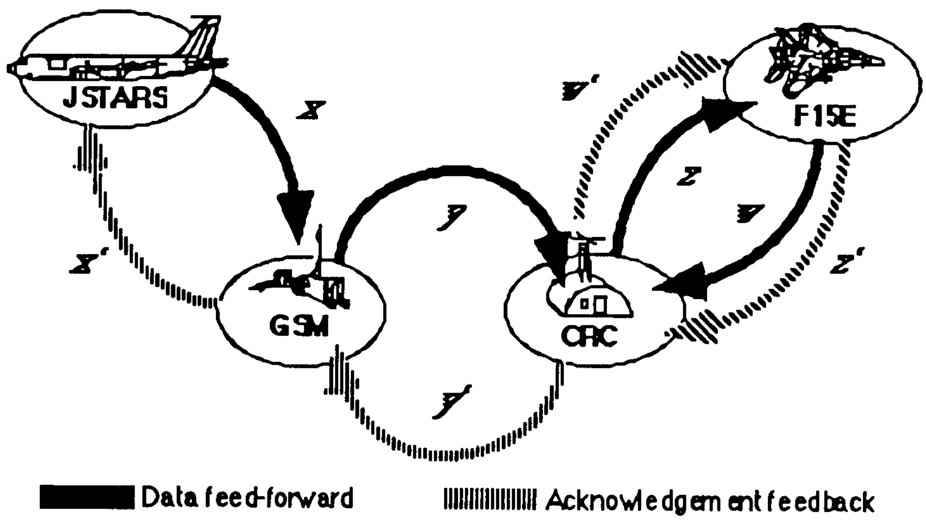

Figure 18: Networking Architecture for the Example Scenarios (Modified for Full Acknowledgement Feedback)

The example simulations were then re-analyzed in terms of this modified messaging protocol. The results are summarized in Table 6 below. With full acknowledgement, the message traffic rate variation between the two scenarios was less than that observed with EADSIM's default / partial acknowledgement (maximum 11.18% versus maximum 20.73%). However, the overall TMD BMC4I message traffic rose significantly.

Table 6: Scenario Messaging (Full Acknowledgement)

Modified Network Architecture
(Full Acknowledgement)

	Wait & Pounce	Immediate Kill	Wait & Pounce	Immediate Kill
	MESSAGES GENERATED		MESSAGES RECEIVED	
JSTARS	35	18	35	18
GSM	70	36	70	36
CRC	58	38	58	38
F15E	23	20	23	20
Total messages:	186	112	186	112
Scenario length (secs):	2814	1524	2814	1524
Average messages/sec	0.066098	0.073490	0.066098	0.073490
Percentage difference in message traffic rates between scenarios:	-10.06 %	+11.18 %	-10.06 %	+11.18 %

Compared to the partial acknowledgement runs, the full acknowledgement scenarios had message traffic rates which were 43.08% higher for the "wait and pounce" case, and 31.76% higher for "immediate kill." With regard to individual units, these increases were distributed as follows:

- *Messages Received.* Under the condition of full acknowledgement, the number of messages received by the GSM increased by 100% in each of the response scenarios. The number of messages received by the F15E grew by 1050% (wait and pounce) and 81.8% (immediate kill).

- *Messages Generated.* Under the condition of full acknowledgement, the number of messages generated by the CRC increased by 2800% (wait and pounce) and 245.5% (immediate kill).

The increases listed above are entirely attributable to one change -- the CRC's need to acknowledge incoming messages from the GSM and the F15E. The burden of these increases is not, however, limited to CRC. The rise in CRC message outputs has the "ripple effect" of raising the message traffic (and message traffic rates) for all corresponding receivers, with the highest such "spin-off" burden propagating "downstream" (to the F15E) for the time-critical "immediate kill" scenario.

Faster coordinated action and heightened communicational integrity are key goals for TMD BMC4I systems. As the earlier EADSIM results (Figure 17; Table 1) illustrated, the additional operational burden entailed in communicating for faster coordinated action ("immediate kill" versus "wait and pounce") can prove substantial. As the subsequent results (Figure 18; Table 6) illustrate, the additional operational burden of increasing communicational integrity in a network of informationally-localized units can be even more substantial. The corresponding cognitive burdens on the human actors in the TMD system are a critical concern requiring human factors inquiry and cognitive engineering solutions. This concern is motivated by the state of current and prospective TMD BMC4I architectures, plus the operational needs of TMD in the age of IW. This concern is in turn sufficient motivation for prioritizing human factors / cognitive engineering projects aimed at enhancing TMD BMC4I for maximum informational effectiveness and communication efficiency.

X. FINAL SUMMARY AND CONCLUSIONS

This document has identified and discussed a set of critical issues arising from current efforts to adapt American military capacities in response to the proliferation of information technologies. These issues concern the means by which large collections of widely-dispersed actors can coordinate themselves to function as an effective and efficient *system of systems*. Current planning and deployment initiatives make wide-area data communications the "skeleton" for future operations at all levels. This reliance on information networking corresponds to emergent interest in information warfare. We have introduced this nascent area, sifted through its definitional tangles, and differentiated its scope into two subareas: IDW and ISW. We have explored how cognitive engineering research can contribute to inducing information dominance (IDW) through more efficient and effective utilization of technology (ISW). This document has presented the foundations for a program of immediate benefit to USAF / DOD efforts in information warfare. Specifically, we have:

- proposed a specific type of solution -- the *common battlespace picture (CBP)* -- for organizing and exploiting theater information assets.
- made a case for the necessity of pursuing *information requirements analyses (IRA's)* addressing IW issues.
- identified and introduced a military command and control device (Boyd's *OODA Loop)* for organizing such work and its results.
- illustrated how an OODA model can be applied to analyze tasks and missions more fully than current practice permits.
- discussed (generally and with respect to specific examples) the manner in which the proposed OODA approach complements and extends relevant research and development capabilities and practices.
- outlined an *integrated cognitive engineering program* which brings together the OODA Model's innovations and existing tools to comprise a comprehensive cognitive engineering suite.

REFERENCES

Adams, M., Tenney, Y., and R. Pew (1995, March). Situation awareness and the cognitive management of complex systems, in *Human Factors*, 37: 1, 85-104.

AJP ACTD (1995, July). *Advanced Joint Planning Advanced Concept Technology Demonstration (AJP ACTD)*. Available WWW: http://dc.isx.com/AJP_ACTD/Section/ProgMgmt/Operational.html#know

Alberts, J. (1995, October). Dominant battlespace knowledge, in Johnson, Stuart E., and Martin C. Libicki (eds.), *Dominant Battlespace Knowledge: The Winning Edge*, Washington, D.C.: National Defense University Press, 72-86.

Arana-Barradas, MSgt L. A. (1995, July 15). Global presence: The new approach, Washington D.C.: Air Force News Service.

Arnett, E. H. (1992). Welcome to hyperwar, *The Bulletin of the Atomic Scientists*, 48: 7, 14-21.

Arquilla, J., and D. Ronfeldt (1993). Cyberwar is coming!, *Comparative Strategy*, 12: 2, 141-165.

Attack Operations Analysis: BMC4I Architectures. Briefing documentation of 18 May 1995.

Bannon, L. (1989). Shared information spaces: Cooperative user support networks, in *Proceedings of the Conference "Mutual Uses of Science and Cybernetics,"* Amsterdam: University of Amsterdam, 12-20.

Bateson, G. (1987). *Steps to an Ecology of Mind*, Northvale, NJ: Aronson.

Boff, K. R. (1987). The tower of Babel revisited: On cross-disciplinary chokepoints in system design. In W. B. Rouse and K. R. Boff (Eds.) *System design: Behavioral perspectives on designers, tools, and organizations* (pp. 83-96). New York: Elsevier.

Boyd, J. R. (1987, August). *A Discourse on Winning and Losing*, Air University Library, Maxwell AFB Report no. MU 43947 (unpublished briefing).

Brachman, R. (1979): On the Epistemological Status of Semantic Networks. In N. V. Findler (Ed.), *Associative Networks: Representation and Use of Knowledge by Computers*, New York: Academic Press.

Brachman, R. (1985): " 'I Lied about the Trees' Or Defaults and Definitions in Knowledge Representation." *AI Magazine*.

Bracken, P. (1995, October). Dominant battlefield awareness, in Johnson, Stuart E., and Martin C. Libicki (eds.). *Dominant Battlespace Knowledge: The Winning Edge*, Washington, D.C.: National Defense University Press, 59-76.

Bush, V. (1945, June). As we may think, *Atlantic Monthly*, no. 176, 101-108.

Campen, A. D. (ed.) (1992), *The First Information War: The Story of Communications, Computers, and Intelligence Systems*, Fairfax VA: AFCEA

International Press.

Campen, A. D. (1995, July). Rush to information-based warfare gambles with national security, *SIGNAL*, 67-69.

Defense Issues, 10: 18. Building an Air Force for the next century. Remarks prepared for delivery by Secretary of the Air Force Sheila E. Widnall and USAF Chief of Staff Gen Ronald R. Fogleman, to the Air Force Association Convention, Orlando, FL, Feb. 23, 1995. Available WWW: http://www.dtic.dla.mil/defenselink/pubs/di95/di1018.html.

Department of the Air Force (1996, October). *Information Warfare*, Air Force Doctrine Document 5 (Second Draft).

DiNardo, R. L., and D. J. Hughes (1995). Some cautionary thoughts on information warfare. *Airpower Journal*, Winter 1995, 1-10.

Doherty, M. (1992). A laboratory scientist's view of naturalistic decision making, in Klein, G., Orasanu, J., Calderwood, R., and C. Zsambok (eds.), *Decision Making in Action: Models and Methods*, Norwood NJ: Ablex, 362-388.

Dominguez, C. (1994). Can SA be defined?, in Vidulich *et al.* (1994), 5-15.

Eco, U. (1976). *A Theory of Semiotics*, Bloomington IN: Indiana University Press.

Ellis, J. (1975). *The Social History of the Machine Gun*, New York: Pantheon Books.

Ely, R. (1995, March). Information Warfare, *Leading Edge*, 4.

Emmett, P. (1994). Software warfare: The militarization of logic, *Joint Forces Quarterly*, Summer 1994, 84-90.

Endsley, M. R. (1988). Design and evaluation for situation awareness enhancement, in *Proceedings of the Human Factors 32nd Annual Meeting , Volume 1,* 97-101. Santa Monica CA: Human Factors Society.

Endsley, M. R. (1991). Situation awareness in an advanced strategic mission, Wright-Patterson AFB OH: Air Force Systems Command Technical Report AL-TR-1991-0083.

Endsley, M. R. (1994). Situation awareness in dynamic human decision making: Theory, in Gilson, R., Garland, D., and J. Koonce (eds.), *Situation Awareness in Complex Systems*, Daytona Beach FL: Embry-Riddle Aeronautical University Press, 1994, 27-58.

Endsley, M. R. (1995, March). Toward a theory of situation awareness in dynamic systems, in *Human Factors*, 37: 1, 32-64.

Engelbart, D., [1988a] A conceptual framework for the augmentation of man's intellect, reprinted in Greif, I. (ed.), *Computer-Supported Cooperative Work: A Book of Readings*, San Mateo CA: Morgan Kaufmann, 1988, pp. 35-65.

Engelbart, D., [1988b] Toward high-performance knowledge workers, reprinted in Greif, I. (ed.), *Computer-Supported Cooperative Work: A Book of Readings*, San Mateo CA: Morgan Kaufmann, 1988, pp. 67-78.

Fogleman, Gen R. R [1995a]. Address to the Armed Forces Communication and

Electronics Association, Washington D.C., April 25 1995.

Fogleman, Gen R. R [1995b]. Address to the Air Force Association Convention, Washington D.C., September 20, 1995.

Gibson, W. (1984). *Neuromancer*, New York: Ace Books.

Gilson, R. (ed.) (1995, March). *Human Factors*, 37: 1. Special issue on situation awareness.

Griffith, S. B. (1963). Introduction to Sun Tzu (1963), 1-56.

Hammond, G. T. (1994). Paradoxes of war, *Joint Forces Quarterly*, Spring 1994, 7-16.

ICAM Architecture Part II-Volume IV - Function Modeling Manual (IDEF0), AFWAL-TR-81-4023, Materials Laboratory, Air Force Wright Aeronautical Laboratories, Air Force Systems Command, Wright-Patterson Air Force Base, Ohio 45433, June 1981.

ICAM Architecture Part II-Volume IV - Function Modeling Manual (IDEF0), AFWAL-TR-81-4023, Materials Laboratory, Air Force Wright Aeronautical Laboratories, Air Force Systems Command, Wright-Patterson Air Force Base, Ohio 45433, June 1981.

ICAM Architecture Part II, Volume V - Information Modeling Manual (IDEF1), AFWAL-TR-81-4023, Materials Laboratory, Air Force Wright Aeronautical Laboratories, Air Force Systems Command, Wright-Patterson Air Force Base, Ohio 45433, June 1981.

Institute for National Strategic Studies (INSS) (1996). *Strategic Assessment 1996: Instruments of U. S. Power*, Washington DC: National Defense University. Available WWW: http://www.ndu.edu/ndu/inss/sa96/sa96cont.html

Jensen, O. E. (1994). Information warfare: Principles of third-wave war, *Airpower Journal*, Winter 1994, 35-43.

Johnson, S. E., and M. C. Libicki (eds.) (1995). *Dominant Battlespace Knowledge: The Winning Edge*, Washington, D.C.: National Defense University Press, October 1995. Text available via WWW at: http://www.ndu.edu:80/ndu/inss/books/dbk/

Joint Chiefs of Staff (1996). *Joint Vision 2010. America's Military: Preparing for Tomorrow*. Washington D.C.: Office of the Chairman, JCS, 1996.

Keegan, J. (1993). *A History of Warfare*, New York: Alfred A. Knopf.

Kirwan, B., and L. Ainsworth (eds.) (1992). *A Guide to Task Analysis*, London: Taylor & Francis.

Klein, G., Orasanu, J., Calderwood, R., and C. Zsambok (eds.) (1992). *Decision Making in Action: Models and Methods*, Norwood NJ: Ablex.

Klein, G., and D. Woods (1992). Conclusions: Decision making in action, in Klein, G., Orasanu, J., Calderwood, R., and C. Zsambok (eds.), *Decision Making in Action: Models and Methods*, Norwood NJ: Ablex, 1992, 404-411.

Kraemer, K., and J. King (1988, June). Computer-based systems for cooperative work

and group decision making, *ACM Computing Surveys*, 20: 2, 115-146.

Krepinevich, A. (1992, July). *The Military Technical Revolution: a Preliminary Assessment*, Office of the Secretary of Defense, Office of Net Assessment.

Krepinevich, A. (1994). Cavalry to computer: The pattern of military revolutions, *The National Interest*, Fall 1994, 30-42.

Lee, A. M., and E. B. Lee (1939). *The Fine Art of Propaganda*, New York: Institute for Propaganda Analysis / Harcourt, Brace and Company.

Lee, J. G. (1994, October). *Counterspace Operations for Information Dominance*, Maxwell AFB AL: Air University Press (Thesis publication).

Leonhard, R. R. (1994). *Fighting by Minutes: Time and the Art of War*, Westport CT: Praeger Publishers.

Libicki, M. C. (1995, May). What is information warfare? Washington DC: National Defense University Strategic Forum Report Number 28, May 1995. Available WWW: http:/ /198.80.36.91/ndu/inss/strforum/forum28.html.

Lipshitz, R. (1992). Converging themes in the study of decision making in realistic settings, in Klein, G., Orasanu, J., Calderwood, R., and C. Zsambok (eds.), *Decision Making in Action: Models and Methods*, Norwood NJ: Ablex, 1992, 103-137.

Llinas, James (SUNY Buffalo / Multisource Inc.), Fusion, Situational Awareness and Information Warfare, briefing presentation to CIWAL, 20 February 1995.

Lum, Zachary A. (1994, August). "Linking the Senses," *Journal of Electronic Defense*, 33-38.

Mann, E. (1994). Desert Storm: The first information war?, *Airpower Journal*, Winter 1994, 4-14.

Mazarr, M. J. (1994). *The Revolution in Military Affairs: A Framework for Defense Planning*. Carlisle PA: Strategic Studies Institute, Army War College.

McKenzie, K. F., Jr. (1995, Summer). Beyond Luddites and magicians: Examining the MTR, *Parameters*, 15-21.

McMillan, G. (1994). Report of the Armstrong Laboratory Situation Awareness Integration (SAINT) Team, in Vidulich *et al.* (1994), 37-47.

Morton, O. (1995, June 10). The information advantage, *The Economist.*, 5-20.

Munro, Neil (1991). *Electronic Combat and Modern Warfare*, New York: MacMillan.

Munro, Neil (1995, July 16). The Pentagon's New Nightmare: An Electronic Pearl Harbor, *Washington Post*. Available WWW: http://vislab-www.nps.navy.mil/~sdjames/pentagon_nightmare.html

Nardi, B. A. (ed.) (1995). *Context and Consciousness: Activity Theory and Human-Computer Interaction*, Cambridge MA: MIT Press.

Norman, D. (1981). Steps toward a cognitive engineering: System images, system friendliness, mental models. Paper presented at Symposium on Models of Human Performance, Office of Naval Research Contractors' Meeting, La Jolla CA:

University of California, San Diego, June 19, 1981.

Norman, D. (1983). Some observations on mental models, in Gentner, D., and A. Stevens (eds.), *Mental Models*, Hillsdale NJ: Lawrence Erlbaum Associates, 1983, 7-14.

Norman, D. (1984). Cognitive engineering principles in the design of human-computer interfaces, in G. Salvendy (ed.), *Human-Computer Interaction*, Amsterdam: Elsevier Science Publishers, 1984, 11-16.

Norman, D. (1986). Cognitive engineering, in Norman, D., and S. Draper (eds.), *User Centered System Design*, Hillsdale NJ: Lawrence Erlbaum Associates, 1986, 31-61.

Norman, D., and S. Draper (eds.) (1986). *User Centered System Design*, Hillsdale NJ: Lawrence Erlbaum Associates.

Norman, D. (1987). Cognitive engineering -- cognitive science, in Carroll, J. (ed.), *Interfacing Thought: Cognitive Aspects of Human-Computer Interaction*, Cambridge MA: MIT Press, 1987, 325-336.

Orasanu, J., and T. Connolly (1992). The reinvention of decision making, in Klein, G., Orasanu, J., Calderwood, R., and C. Zsambok (eds.), *Decision Making in Action: Models and Methods*, Norwood NJ: Ablex, 1992, 3-20.

Owens, Adm W. A. [1995a]. The emerging system of systems, *Naval Institute Proceedings*, May 1995, 35-39.

Owens, Adm W. A. [1995b]. Keynote Address, 1995 Military Operations Research Society Symposium, Annapolis MD: US Naval Academy, June 1995.

Owens, Adm W. A. [1995c] Introduction, in Johnson, Stuart E., and Martin C. Libicki (eds.). *Dominant Battlespace Knowledge: The Winning Edge*, Washington, D.C.: National Defense University Press, October 1995, 3-18.

Peirce, C. S. (1933) *Collected Papers*. Edited by Charles Hartshorne and Paul Weiss. Cambridge MA: Harvard University Press.

Powell, C. L. (1992, July). Information-age warriors, *BYTE*, 370.

RAND Corporation (1995a). Information Warfare: A Two-Edged Sword, *Rand Research Review*, Vol. 19:2 (Fall 1995), Information War and Cyberspace Security. Available WWW: http://www.rand.org/publications/RRR/RRR.fall95.cyber/infor_war.html

RAND Corporation (1995b). Related Reading - An IW Bibliography, *Rand Research Review*, Vol. 19:2 (Fall 1995), Information War and Cyberspace Security. Available WWW: http://www.rand.org/publications/RRR/RRR.fall95.cyber/index.html

RAND Corporation (1995c). Keeping Information Warfare in Perspective, *Rand Research Review*, Vol. 19:2 (Fall 1995), Information War and Cyberspace Security. Available WWW: http://www.rand.org/publications/RRR/RRR.fall95.cyber/perspective.html

RAND Corporation (1995d). The fly on the wall and the Jedi Knight, Research Brief (abstract) for Hundley, Richard O,. and Eugene C. Gritton, *Future Technology-Driven Revolutions in Military Operations: Results of a Workshop*, RAND Report DB-110-ARPA, 1995. Available WWW: http://www.rand.org:/publications/RB/RB7104/RB7104.html

Rasmussen, J. (1986). *Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering*, North-Holland Series in System Science and Engineering, Vol. 12, New York: North-Holland (Elsevier Science Publishers).

Rasmussen, J., A. M. Pejtersen, and L. P. Goodstein (1994). *Cognitive Systems Engineering*, New York: Wiley, 1994.

Rokke, E. (Lt Gen USAF), Foreword to Johnson & Libicki (1995), ix.

Rona, T. P. (1976, July). Weapon systems and information war, Seattle: Boeing Aerospace Co. research report.

Ryan, D. E., Jr. Implications of information-based warfare, *Joint Forces Quarterly*, Autumn/Winter 1994-95, 114-116.

Shalikashvili, Gen John (Chairman, JCS) (1996). *Posture Statement*, presentation to the 104th Congress Committee on Armed Services, United States Senate, March 5, 1996. Text available WWW: http://www.dtic.mil/jcs/chairman/posture/posture.html

Simpson, J. M. (1980, May/June). Doing things the same or differently: An alternative approach to the study of conflict, *Air University Review*, 31: 4, 88-93.

Stiffler, D. (1987, April). *Exploiting Situational Awareness Beyond Visual Range*, Maxwell AFB AL: Air Command and Staff College report 87-2370.

Stiffler, D. (1988, Summer). Graduate Level Situation Awareness, *USAF Fighter Weapons Review*, 36: 2, 15-20.

Sullivan, Gen G. R., and Col J. M. Dubik (1994, April). War in the information age, *Military Review*, 46-62.

Sun Tzu (1963). *The Art of War*. Translated by S. B. Griffith. London: Oxford University Press.

Szafranski, R. (1994, November). Harnessing battlefield technology: Neocortical warfare: The acme of skill, *Military Review*.

Szafranski, R. (1995, Spring). When waves collide: Future conflict, *Joint Forces Quarterly*.

Szafranski, R. (1995, Spring). A theory of information warfare: Preparing for 2020, *Airpower Journal*, IX: 1 (Spring 1995), 56-65. Available WWW: http://www.cdsar.af.mil/apj/szfran.html

Toffler, A., and H. Toffler (1980). *The Third Wave*, New York: Bantam Books.

Toffler, A., and H. Toffler (1990). *Power Shift*, New York: Bantam Books.

Toffler, A., and H. Toffler (1991, May). War, wealth, and a new era in history, *World Monitor*, 4: 5, 46-52.

Toffler, A., and H. Toffler (1993). *War and Anti-War: Survival at the Dawn of the 21st Century*, Boston MA: Little, Brown and Co.

U.S. Air Force (1995). Air Force Doctrine Document (AFDD) 5: Information Warfare, Preliminary Draft.

U.S. Air Force Scientific Advisory Board (1995, December). *New World Vistas: Air and Space Power for the 21st Century.* Summary material available via WWW at http://web.fie.com/htdoc/fed/afr/sab/any/text/any/vistas.htm

Vidulich, M. (1994). Cognitive and performance components of situation awareness, in Vidulich *et al.* (1994), 17-28.

Vidulich, M., C. Dominguez, E. Vogel, and G. McMillan (1994, June). *Situation Awareness: Papers and Annotated Bibliography (U),* Dayton OH: USAF technical report AL/CF-TR-1994-0085.

Waller, D. (1995, August 21). Onward cyber soldiers, *TIME*, 38-46.

Waltz, E., and J. Llinas (1990). *Multisensor Data Fusion* , Boston: Artech House.

Wetzel, M. and S. Kowall (1994, November). *Theater Air Defense: Attack Operations & Active Defense for Theater Missile Defense*, Draft report of Air Combat Command, Directorate for Requirements, Aerospace Control Division.

Wertsch, J. V. (translator / ed.) (1981).*The Concept of Activity in Soviet Psychology*, Armonk, NY: M.E. Sharpe.

Widnall, S. E. (1995, September 21). Widnall says USAF is ready for IW mission, *Aerospace Daily* , 445.

Widnall, S. E., and Gen R. R. Fogleman (1995, October). *Cornerstones of Information Warfare*, Washington D.C.: Dept. of the Air Force.

Wohl, J. G. (1980). *Battle Management Decisions in Air Force Tactical Command and Control*, Bedford MA: MITRE Corporation technical report ESD-TR-80-123, May 1980.

Wohl, J. G. (1981, September). Force management requirements for Air Force tactical command and control, *IEEE Transactions on Systems, Man, and Cybernetics*, SMC-11: 9 (September 1981), 618-639.

Wohl, J. G., E. E. Entin, and J. S. Eterno (1983, January). Modeling human decision processes in command and control, Alphatech, Inc. technical report TR-137.

APPENDIX A:

GLOSSARY

This appendix contains a summary collection of definitions for the terminology used throughout this document. It also recounts most of the quoted material drawn from the literature, so as to provide a "quick reference" for the reader who wishes to check on a term, but who would prefer to avoid scanning through the entire text.

acme of skill -- Taken from Sun Tzu's *The Art of War*:"...to subdue an adversary without killing him." (quoted in Szafranski, 1995, p. 57)

act -- Synonym for "Action" -- used to denote the final phase of the OODA Loop (Boyd, 1987).

action -- The fourth and final phase of the OODA Loop (Boyd, 1987). In this phase the result(s) of the Decide / Decision phase are enacted, after which the system proceeds to the next iteration of its OODA Loop through a subsequent Observe / Observation phase.

battlespace -- the field of military operations circumscribed by the aggregate of all spatial (e.g., geographic range, altitude) and virtual (e.g., communicational connectivity) dimensions in which those operations are realized.

BMC4I -- Battle(-space) Management Command, Control, Communications, and Intelligence. Briefly stated, the overall label for those components and processes comprising the "nervous system" of a modern military force in a theater of operations.

"...the planning, tasking, and control of the execution of missions through an architecture of sensors, communications, automation, and intelligence support." (Wetzel and Kowall, 1994, p. 2)

C2 attack -- "Any action against any element of the enemy's command and control system." (Widnall & Fogleman, 1995)

C2 Counterwar -- Presumed synonym for Command and Control Counterwar (cf. Jensen, 1994, p. 35).

C2W -- "Acronym for ...command and control warfare..." (Stein, 1995, p. 31). This term is not synonymous with *information warfare / IW* (cf. Szafranski, 1995).

C3I -- Command, Control, Communications, and Intelligence.

C4I -- Command, Control, Communications, Computers, and Intelligence.

command and control -- "The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission." (Widnall & Fogleman, 1995)

command and control counterwar -- Apparently a synonym for *IW / knowledge*

war / *third-wave war* (cf. Jensen, 1994, p. 35). This would be distinct from *C2W* (*Command and Control Warfare*), according to Szafranski (1995), who considers *C2W* and *IW* to be entirely distinct concepts.

command and control warfare -- (Acronym = *C2W*). Has as its aim "...to use physical and radio-electronic combat attacks against enemy information systems to separate enemy forces from enemy leadership." (Szafranski, 1995, p. 65, footnote 1).

"The integrated use of operations security, military deception, psychological operations, electronic warfare and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions." (Campen, 1995, p. 68 attributed to Joint Chiefs of Staff MOP-30)

The term replacing the earlier *command, control and communications countermeasures* (cf. Campen, 1995, p. 68)

With reference to the *OODA Loop*, C2W can be characterized as targeting the transition between the D(-ecision) and A(-ction) phases.

command, control and communications countermeasures -- The phrase replaced by the term *command and control warfare* (cf. Campen, 1995, p. 68).

common battlespace picture (CBP) -- CIWAL's term for a shared information asset providing all actors in a theater SOS with a mutually accessible reference point on the status and dynamics of their operations.

counterinformation -- "Actions dedicated to controlling the information realm." (Widnall & Fogleman, 1995)

Activities which "... establish information control and enable all other activities. Combined with counterair and counterspace, counterinformation creates an environment where friendly forces can conduct operations with some degree of freedom of action, while simultaneously denying the adversary the ability to conduct those operations against friendly forces. Counterinformation seeks to establish a desired degree of information superiority by destroying or neutralizing enemy information functions." (Department of the Air Force, 1996, p. 4)

Also spelled *counter-information* (cf. Gen Joe Ralston, quoted in Arana-Barradas, 1995)

cyber medium -- Apparently a synonym for *cyberspace* -- i.e., the realm of information activities and entities (Defense Issues 10:18).

cyberspace -- Metaphorically, the realm of information activities and entities resident, so to speak, in data networks and accessible via computers.

"...the global world of internetted computers and communication systems" (RAND, 1995d).

"The notional environment within which electronic communications occurs. The space of virtual reality." (Campen, 1995, p. 68)

The term was coined by the science fiction author William Gibson (1984). This is the layman's term to which a variety of IW authors refer using labels such as: *cyber medium, infosphere, datasphere, virtual realm,* and *virtual battlespace.*

cyberwar -- A RAND Corporation synonym for *information warfare* (Grier, 1995, p. 37)

In contrast, the term is also used as a synonym for *netwar* -- a superset of *IW* (cf. Szafranski, 1995, p. 58).

Libicki (1995) calls cyberwar "combat in the virtual realm."

Arquilla and Ronfeldt (1993) use "cyberwar" to designate "knowledge-related conflict at the military level" and limit their application of the term to IW strategies "...of the sort that might be used against insurgents by a high-technology opponent..." (cited in Morton (1995)). For these authors, cyberwar is contrasted with *netwar* (taken in the sense of non-military information warfare).

A synonym for automated warfare: "...in which robots do much of the killing and destroying without direct instructions from human operators. The weapons would be 'autonomous' ..." (Arnett, 1992, p. 15)

DBA -- Acronym for *dominant battlespace awareness.*

DBK -- Acronym for *dominant battlespace knowledge.*

decision -- The third phase in the OODA Loop (cf. Boyd, 1987). In this phase, the result(s) of the Orient / Orientation phase provide the basis for selecting response(s) to be fed forward to effectuation in the Act / Action phase.

decide -- Synonym for "Decision" -- used to denote the third of the four phases in the OODA Loop.

defensive counterinformation -- "Actions protecting our military information functions from the adversary." (Widnall & Fogleman, 1995) Cf. *defensive information warfare.*

defensive information warfare (defensive IW) -- Those tactics intended "...to protect our ability to conduct information operations. ... Traditional defensive IW operations include physical security measures and encryption. Nontraditional actions will range from antivirus protection to innovative methods of secure data transmission." (Joint Chiefs of Staff, 1996, p. 16). Cf. *defensive counterinformation.*

direct information warfare -- "Changing the adversary's information without involving the intervening perceptive and analytical functions." (Widnall & Fogleman, 1995)

dominant battlespace awareness (DBA) -- A term applied to connote own-system advantage with respect to sensor / reconnaissance / intelligence data in a particular battlespace. Cf. Owens (1995a; 1995b).

dominant battlespace knowledge (DBK) -- A term applied to connote the own-system understanding and capacity for action deriving from (dominant) battlespace

awareness.

"...namely, the ability to *understand* what we see and *act* on it decisively" (Rokke, 1995, p. ix).

Derives from "...merging our increasing capacity to gather real-time, all-weather information continuously with our increasing capacity to process and make sense of this voluminous data..." (Owens, 1995c, p. 7)

first-wave war(fare) -- Cf. Toffler & Toffler (1993). The term for the mode or character of war(fare) exemplified in primitive, pastoral, and agricultural societies and dating from prehistory. This is Toffler's category corresponding to *pre-industrial war(fare)* or *primitive war(fare)*, as those terms are colloquially used.

fog of war -- the aggregate of factors which reduce or preclude situational certainty in a battlespace.

full spectrum dominance -- A concept outlined in the document *Joint Vision 2010* (Joint Chiefs of Staff, 1996), denoting "...the capability of our Armed Forces to dominate any opponent across the range of military operations" (Shalikashvili, 1996). Such dominance is to be achieved through "...leveraging today's high quality forces and force structure with leading-edge technology to attain better command, control and intelligence and to implement new operational concepts -- dominant maneuver, precision strike, full dimensional protection, and focused logistics." (*Ibid.*) Each of these four capabilities are in turn predicated on *information superiority* .

hyperwar -- A term (attributed to "Air Force planners") describing the notion that "...war is becoming unimaginably -- and unmanageably -- fast." (Arnett, 1992, p. 15)

IBW -- (1) Acronym for *information-based warfare* (Ryan, 1995).

(2) Acronym for *intelligence-based warfare* (Libicki / National Defense University Strategic Forum 28, 1995).

IDW -- Acronym for *information dominance warfare.*

indirect information warfare -- "Changing the adversary's information by creating phenomena that the adversary must then observe and analyze." (Widnall & Fogleman, 1995)

industrial warfare -- Cf. Toffler & Toffler (1993). The term for the class or character of war / warfare exemplified from the 18th Century through to the present. Synonymous with *Second-Wave War(fare).*

information -- The problematical concept spanning the gap between "data" (in the sense of "signals" or "bytes" -- i.e., discrete units of channel perturbation) and "knowledge" (in the sense of integrated capacity for effective action in a specified domain of operations). Cf. Arquilla and Ronfeldt (1993) on information as "something more than data but less than knowledge." As generally used in the IW literature, information is taken in the colloquial sense to denote that portion of

available data which provides or imputes "meaning" (another very problematical concept). This is well-illustrated by the claim that information constitutes the "...content or meaning of a message" and obtains its status by being "...'any difference that makes a difference' ." (Szafranski, 1995, p. 57; cf. Bateson, 1987, for the coining of the latter phrase). In this sense, "information" carries a connotation of interpretability with respect to an observer / receiver, as well as a connotation of integrability and utility with respect to an actor and a scenario. Cf. Widnall and Fogleman (1995, p. 2), who define the term as "data and instructions" in the sense of "...perceived phenomena (data) and the instructions required to interpret that data and give it meaning."

This is distinct from the term's formal usage in *information theory* (cf. Shannon and Weaver, 1948), wherein "information" is a quantifiable metric of uncertainty reduction. Put another way, this more formal usage pertains to the features of a channel or the form of a message (in contrast with Szafranski's comment above). As such, the formal version of the term doesn't address the situational factors of interpretability, integrability, or utility as delineated above. Allusion to these factors in the IW literature is not universal, and some authors tilt toward the more formalized view by claiming (e.g.) that information "...is passive and always exists (at least in the abstract) whether anyone pays attention to it or not." (Mann, 1994, p. 9). For the purposes of this discussion, this conflicting formal viewpoint is admitted only to the extent it supports leveraging information channels as vehicles (e.g., *C2W*). The earlier (Szafranski / Bateson) version is the one applied in discussions of leveraging the content and throughput of those channels (e.g., for *information dominance*).

information age warfare -- That subset of warmaking which "...uses information technology as a tool to impart our combat operations with unprecedented economies of time and force." (Widnall & Fogleman, 1995, p. 2 -- exemplified (*Ibid.*, footnote 1) by a cruise missile (cf. Owens (1995a) on precision force projection). Cf. Rona's (1976) *information war*.

information assurance -- As defined in Department of the Air Force (1996), one of two major subcomponents of information warfare. Information assurance "... consists of measures to enhance and protect friendly information and functions." (p. 6) Information assurance is in turn decomposed into *information enhancement* and *information protect(-ion)*.

information attack -- "Directly corrupting information without visibly changing the physical entity within which it resides." (Widnall & Fogleman, 1995, p. 6) In the wake of an information attack "...an information function is indistinguishable from its original state except through inspecting its data or instructions." (*Ibid.*)

information-based warfare -- Synonym for *information warfare* (cf. Ryan, 1995). "An approach to armed conflict focusing on managing and using information in all its

forms and at all levels to achieve a decisive military advantage, especially in the joint and combined environment." (Campen, 1995, p. 68).

Acronym = *IBW* (cf. Ryan, 1995). NOTE: The IBW acronym is also used for *intelligence-based warfare.*

information dominance -- In warfare, an operational advantage obtained through superior effectiveness of informational activity (acquisition and processing of data, information, and/or knowledge), to the extent that this advantage is demonstrated in practice through superior effectiveness of instrumental activity.

Information dominance has as its true purpose "...to provide an exploitable knowledge dominance." (Mann, 1994, p. 9)

According to Lee (1994), the concept dates back to Soviet military theorization of the late 1970's. They saw "information dominance" as a potential outcome of the USA's technological superiority in IT -- a superiority considered to constitute a *military technical revolution.* He cites Krepinevich (1992, p. 14) as the source.

"..a condition in which a nation possesses a greater understanding of the strengths, weaknesses, interdependencies, and centers of gravity of an adversary's military, political, social, and economic infrastructure than the enemy has on friendly sources of national power." (Lee, 1994, p. 3, citing Krepinevich, 1992, p. 22)

information dominance warfare (IDW) -- the subcategory of information warfare (IW) aimed at leveraging data, information, and knowledge to tactical and strategic advantage, as opposed to leveraging the media, channels, and vehicles of information transfer and/or processing. Cf. Widnall & Fogleman's (1995) definition for *IW.* The goal of IDW is to achieve *information dominance.*

information enhancement (IE) -- One of two major subcomponents of *information assurance* -- specifically, "... the organized network of information functions that enhance force employment ... Information enhancement entails the development of information functions that enhance total force effectiveness. This objective is fulfilled by activities involving the acquisition, transmission, storage, or transformation of information that enhance the employment of military forces." (Department of the Air Force, 1996, p. 7)

information function -- "Any activity involving the acquisition, transmission, storage, or transformation of information." (Widnall & Fogleman, 1995)

information operations (also *Information Ops*) -- "Any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces." (Widnall & Fogleman, 1995)

"Our information management capacity will leverage our ability to pinpoint an adversary's centers of gravity. And with this kind of information we'll have a whole new discipline called information operations that will play a critical role before, during and after any crisis." (Defense Issues 10:18, 1995)

information ops -- Synonym for *information operations* (Defense Issues 10:18,

1995)

information protect (IP) -- One of two major subcomponents of *information assurance* which "... seeks to provide the requisite security critical to the military's ability to conduct operations. Information protection ensures availability, integrity, authenticity, and confidentiality of information. The information environment protection process involves determining the scope (what to protect based on the value of information) and the standards for protection. Information protect activities occur within the context of four interrelated processes: information environment security, attack detection, attack response, and capability restoration." (Department of the Air Force, 1996, p. 11). Sometimes referred to as "information protection" (*Ibid.*)

information realm -- A commonly-used term to denote the virtual space of data networks, their contents, and their commerce. Related terms include: *infosphere, cyberspace, datasphere*, and *virtual realm* (Libicki, 1995).

information superiority -- "The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Information superiority will require both offensive and defensive information warfare (IW)." (Joint Chiefs of Staff, 1996, p. 16).

information systems warfare (ISW) -- the subcategory of information warfare (IW) aimed at leveraging media, channels, and vehicles of information transfer and/or processing to tactical and strategic advantage. Cf. Widnall & Fogleman's (1995) *information age warfare.*

information war -- A term used by Rona (1976) to connote activities "intertwined with, and superimposed on, other military operations" exploiting data and information in support of traditional military tasks such as command and control. Cf. Widnall & Fogleman's (1995) *information age warfare.*

"Manipulative, disruptive or destructive actions taken covertly or overtly during peacetime, crisis or war against societal, political, economic, industrial or military electronic information systems." (Campen, 1995, p. 68, as *information war(fare)*).

information warfare (abbreviated **IW**)-- The broad class of activities aimed at leveraging data, information, and knowledge in support of military goals. Subcategories of information warfare can be differentiated into two general classes: (a) those aimed at leveraging the vehicles of information transfer / processing (*information systems warfare -- ISW*) and (b) those aimed at leveraging the informative content or effect of such systems, whether those targeted by (a) or not -- *information dominance warfare (IDW).*

"...views information itself as a separate realm, potent weapon, and lucrative target." (Widnall & Fogleman, 1995, p. 2)

"Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military

information functions." (Widnall & Fogleman, 1995)

"...in its largest sense, is simply the use of information to achieve our national objectives." (Stein, 1995, p. 32)

"...can be seen as societal-level or nation-to-nation conflict waged, in part, through the worldwide internetted and interconnected means of information and communication." (Stein, 1995, p. 32)

"...in its most fundamental sense, is the emerging 'theater' in which future nation-against-nation conflict at the strategic level is most likely to occur." (Stein, 1995, p. 32)

"...may be the theater in which 'operations other than war' are conducted, especially as it may permit the United States to accomplish some important national security goals without the need for forward-deployed military forces in every corner of the planet." (Stein, 1995, p. 32)

"...in its essence, is about ideas and epistemology -- big words meaning that information warfare is about the way humans think and, more importantly, the way humans make decisions." (Stein, 1995, p. 32)

"...is about influencing human beings and the decisions they make." (Stein, 1995, p. 32)

"...at the strategic level is the 'battle off the battlefield' to shape the political context of the conflict." (Stein, 1995, p. 33)

(With respect to establishing IW doctrine:) ...assume that information warfare is warfare in the information realm as is air warfare in the air and space realm. (Stein, 1995, p. 38)

"...sometimes is erroneously referred to as command and control warfare, or C2W." (Szafranski, 1995, p. 65, footnote 1).

"...is a much larger set of activities [than C2W] aimed at the mind and will of the enemy." (Szafranski, 1995, p. 65, footnote 1).

"...is a form of conflict that attacks information systems directly as a means to attack adversary knowledge or beliefs." (Szafranski, 1995, p. 58).

"...can be prosecuted as a component of a larger and more comprehensive set of hostile activities -- a netwar or cyberwar -- or it can be undertaken as the sole form of hostile activity." (Szafranski, 1995, p. 58).

Defined to be a possible component (therefore a partial subset?) of *netwar* and/or *cyberwar* (cf. Szafranski, 1995, p. 58).

"...is hostile activity directed against any part of the knowledge and belief systems of an adversary." (Szafranski, 1995, p. 58).

(For USAF:) "...is any action that we may take to deny, exploit, corrupt, or destroy an enemy's information and its functions, while protecting those actions, those functions, for ourselves." (Maj Gen Robert E. Linhard, USAF director of plans in the office of the deputy chief of staff for Plans and Operations, quoted in Grier,

1995, p. 36. NB: cf. Ralston in Ely, 1995)

(For USAF:) "...is any action to deny, exploit, corrupt or destroy the enemy's information and its systems; while protecting against those actions; and exploiting our own information operations." (Gen Joe Ralston, Vice Chairman of the Joint Chiefs of Staff, quoted in Ely, 1995, p. 4. NB: cf. Linhard in Grier, 1995)

"Manipulative, disruptive or destructive actions taken covertly or overtly during peacetime, crisis or war against societal, political, economic, industrial or military electronic information systems." (Campen, 1995, p. 68, as *information war(fare)*).

Is best explained with reference to A. and H. Toffler's books (cf. Jensen, 1994).

Is not effectively addressed with the principles and tactics of industrial warfare (cf. Jensen, 1994, p. 37 ff.).

At a minimum, "... means the emergence of greatly improved methods of command, control, and communications." (Grier, 1995, p. 35)

"...will be characterized by weapon accuracy and lethality far surpassing that of today's laser-guided bombs and missiles. Situational awareness -- whether it pertains to air or ground combat -- would be extremely exact." (Grier, 1995, p. 35)

infosphere -- Apparent synonym for *cyberspace* -- the *information realm* (Stein, 1995, p. 38).

The term is used by Powell (1992) to connote the informational dimension or subcomponent of the battlespace.

infowar -- Apparent synonym for *information warfare* (cf. Waller, 1995).

instrumental dominance -- (as opposed to *information dominance*). The advantage obtained through superior physical force projection, without regard to or reliance upon any corresponding advantage in relevant informational activities.

intelligence-based warfare -- Warfighting characterized by rapid and effective acquisition and application of intelligence data. (cf. Libicki, 1995). Acronym = *IBW*. NOTE: The "IBW" acronym is also used for *information-based warfare*.

IP -- Acronym for *information protect(-ion)*.

ISW -- Acronym for *information systems warfare*.

IW -- Acronym for *information warfare*

knowledge -- The state or mechanism(s) ascribed to a system to explain complex mediation between effective acquisition of data from, and effective action in, an operational environment. This approach to knowledge explicitly ties it to the processes of both eduction and enaction with respect to the given operational environment, and hence links it to one or more specific actors in that given domain. These connections -- the ones critical to treating "knowledge" as a feature of interest in analyzing the *OODA Loop* -- explain the IW literature's claims that knowledge "...is active and must be possessed if it is to exist -- let alone be useful." (Mann, 1994, p. 9).

knowledge-based warfare -- "The ability of one side to obtain essential and key

elements of truth while denying these same elements of truth to the other side. It is based on Sir Winston Churchill's premise that 'truth (knowledge) is the most precious commodity in warfare.' The key attributes of knowledge-based warfare are timely, high fidelity, comprehensive, synthesized, and visual data. The end game is a complete "pictorial" representation of reality that the decision maker can tune to his/her unique needs at any given time. This picture must include both "blue" and "red" data, although this ACTD concentrates on the provision of "blue" data only." (AJP ACTD, 1995)

knowledge dominance -- In warfare, an operational advantage (vis a vis an adversary) in exploiting information to guide effective action.

This is the goal of *information dominance* (Mann, 1994, p. 9)

knowledge war -- A synonym for *IW* or *Third-Wave War* (cf. Jensen, 1994, p. 35).

military information function -- "Any information function supporting and enhancing the employment of military forces." (Widnall & Fogleman, 1995) Cf. same authors' definition for *information function.*

military technical revolution -- A term from Soviet military theorization of the late 1970's. It denotes the phenomenon where "...extreme transformations in warfare occurred as a result of the exploitation of technology." (Lee, 1994, p. 3, credited to Krepinevich, 1992, p. 3) The Soviets "...saw the operational and organizational innovations resulting from the exploitation of the technology as defining a military technical revolution." (*Ibid.*). Abbreviated "MTR."

MTR -- Acronym for *military technical revolution.*

netwar -- A synonym for *cyberwar* (cf. Libicki, 1995 -- "conflict in the virtual realm") A superset of *information warfare* (cf. Szafranski, 1995, p. 58).

Arquilla and Ronfeldt (1993) use the term more specifically, stating it is "Societal-level ideational conflicts waged in part through internetted modes of communication" and that it "applies to societal struggles most often associated with low intensity conflict by non-state actors, such as terrorists, drug cartels, or black market proliferators of weapons of mass destruction." They apply this version of the term to categorize tactics aimed at information dominance (cf. Morton, 1995).

O-O-D-A Loop (also *OODA Loop*)**--** Observation, Orientation, Decision, Action loop (cited by many and ascribed to Boyd, 1987). See definition under the primary spelling (OODA).

observation -- The first O in the OODA loop (cf. Boyd, 1987, and a variety of authors who cite him). In this phase, the system acquires, accretes, and compiles data about its operational environment. This data is fed forward to the Orient / Orientation phase for analysis and integration.

observe -- A synonym for "Observation" -- used to denote the first of the four phases in the OODA Loop.

offensive counterinformation -- "Actions against the adversary's information

functions." (Widnall & Fogleman, 1995) Cf. *offensive information warfare*.

offensive information warfare (offensive IW) -- Tactics which "...will degrade or exploit an adversary's collection or use of information. It will include both traditional methods, such as a precision attack to destroy an adversary's command and control capability, as well as nontraditional methods such as electronic intrusion in an information and control network to convince, confuse, or deceive enemy military decision makers." (Joint Chiefs of Staff, 1996, p. 16). Cf. *offensive counterinformation*.

OODA Loop (also *O-O-D-A Loop*) -- Observation, Orientation, Decision, Action Loop (cited by many and ascribed to Boyd, 1987). Taken to describe a single iteration of the cycle proceeding from data acquisition, through information integration and decision making, to enaction of a response. Disruption or other damage to the OODA loop (cf. Mann, 1994, on Desert Storm) is a common way of portraying the goal and/or main effect of IW. Also spelled O-O-D-A (per Boyd quote in Mann, 1994).

Orient -- A synonym for "Orientation" -- used to denote the second of the four phases in the OODA Loop.

orientation -- cf. OODA loop (Orientation is the second 'O').

"...an interactive process of many-sided implicit cross-referencing projections, empathies, correlations, and rejections that is shaped by and shapes the interplay of genetic heritage, cultural tradition, previous experiences, and unfolding circumstances." (Boyd, 1987, p. 211)

This phase, "...as the repository of our genetic heritage, cultural tradition, and previous experiences -- is the most important part of the O-O-D-A loop since it shapes the way we observe, the way we decide, the way we 'act'. " (Boyd, 1987, p. 222, quoted in Mann, 1994, pp. 8-9). In this phase, the data fed forward from the Observe / Observation phase is "digested" -- i.e., semantically analyzed and integrated into the system's operant description of its status with respect to its field of operations. The results of the Orient / Orientation phase feed forward to provide the foundation for the Decide / Decision phase.

postindustrial warfare -- Synonym for *IW* (cf. Mann, 1994, p. 13). Cf. *information warfare, cyberwar, knowledge war, Third-Wave war.*

pre-industrial warfare -- Synonym for *First-Wave War(fare)* (cf. Toffler & Toffler, 1993).

Revolution in Military Affairs -- Current term for the transformations driven by the proliferation of IT as tools for optimizing military operations and weapons of military utility. Acronym = *RMA*. The current RMA is an instance of a *military technical revolution (MTR)*.

RMA -- Acronym for *Revolution in Military Affairs.*

SA -- Acronym for *situation awareness.*

second-wave war(fare) -- A synonym for *industrial warfare* -- the mode of warfare characteristic of nation states as they developed during the Enlightenment, through the Industrial Revolution, and on through the 20th Century. The allusion is to Toffler's "Second Wave" of economic activity, typified by mass production and populations integrated at the national level.

shared situation awareness -- The collective perception, comprehension, and projection of environmental elements among a set of actors. Acronym = *SSA*.

situation awareness -- "...the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future." (Endsley, 1988, p. 97). Acronym = *SA*.

SOS -- Acronym for *system of systems* (cf. Owens, 1995a)

SSA -- Acronym for *shared situation awareness.*

system of systems -- A term used by Admiral W. A. Owens (1995a) to denote collective (e.g., theater-wide) forces and players operating as an integrated whole. Acronym = *SOS*.

TBM -- (1) Theater ballistic missile. (2) Theater battle(space) management.

TEL -- Acronym for a missile's mobile *transporter / erector / launcher.*

third-wave war(fare) -- A synonym for *IW* or *knowledge war* (cf. Jensen, 1994, p. 35).Cf. Toffler & Toffler (1993). The allusion is to Toffler's "Third Wave" of economic activity, which concentrates on information and knowledge as raw material and product. According to Toffler & Toffler (1993), this three-tiered economic / political model was a major influence on the DOD thinkers whose work led to today's interest in IW.

TMD -- Theater Missile Defense.

virtual battlespace -- "...the 'ether' occupied by communications impulses, databases, and computer codes." (Grier, 1995, p. 36) In this usage, the term is synonymous with *cyber medium, cyberspace, infosphere.*

virtual realm -- As used by Libicki (1995), a synonym for *information realm* or *cyberspace.*

war -- An event characterized by the open, total, and (relatively) unrestricted prosecution of warfare by lethal means. As such, war "...is not synonymous with warfare" (Szafranski, 1995, p. 57).

warfare -- "...the set of all lethal and non-lethal activities undertaken to subdue the hostile will of an adversary or enemy." (Szafranski, 1995, p. 57). The distinction between this and *war* ties into Szafranski's delineation of information warfare as an activity which could / should be conducted outside the situational frame of war itself.

APPENDIX B:

INTERNET IW RESOURCES

It seems appropriate that the best and most timely source of data on the emergence and evolution of IW issues would be the Internet -- the same thing which has motivated much of the interest in military aspects of cyberspace. The following is but a brief listing of resources available in the Internet (via the World Wide Web, or WWW). The first section lists general compilations of materials and / or pointers to such materials. The second section lists specific documents or sources which have proven useful in compiling this technical report.

B.I. General Resources

2025: Final Report

The USAF Chief of Staff directed that a study of Air Force opportunities and potentials be drafted. This work was mainly conducted through the Air University at Maxwell AFB, Alabama. The summary documentation on the results can be accessed via WWW at:

http://www.au.af.mil/au/2025/

***Airpower Journal*, National Air University, Alabama.**

Many of the papers cited in this report come from the last few years' issues of *Airpower Journal*. The journal makes its articles available via WWW at:

http://www.cdsar.af.mil/air-chronicles.html

Defense Issues

The DOD journal *Defense Issues* can be accessed online at:

http://www.dtic.dla.mil/ defenselink/pubs/di-index.html

Infowar.com

Winn Schwartau (author of the popular book *Information Warfare*) and his organization have recently established a large (and rapidly growing) Web site on IW and related security issues at:

http://www.infowar.com/

Institute for the Advanced Study of Information Warfare (IASIW)
This is an academic site specifically dedicated to IW issues. This site is a major "nexus" of pointers to IW-related Internet resources.

http://psycom.net/iwar.1.htm

New World Vistas: Air and Space Power for the 21st Century
This document is a comprehensive forecast of future military trends assembled under the aegis of the U. S. Air Force's Scientific Advisory Board (SAB). The summary volume, which provides an overview of the entire work, can be accessed via WWW at either of two sites:

http://www.plk.af.mil/ORG_CHART/XP/XPB/nwvistas.html

http://web.fie.com/htdoc/fed/afr/sab/any/text/any/vistas.htm

Rucci, Antonio A.: Information Warfare.
Mr. Rucci is a private individual who in early 1996 established a compendium of IW-related pointers on his personal WWW page. Besides illustrating the potential for individual initiative in cyberspace, his collection rivals any to be found on the Internet.

http://www.serve.com/ruccia/iw.html

B.II. Specific Resources (Papers, Articles, etc.)

Arquilla, John, and David Ronfeldt, Cyberwar is coming!, *Comparative Strategy*, Volume 12 (1993), no. 2, pp. 141-165. Text available via WWW at:

gopher://gopher.well.sf.ca.us:70/00/Military/cyberwar

BBC, *The I-Bomb*, documentary discussion, transcript available via WWW

http://helios.njit.edu:1994/cgi-bin/contrib/interdependence/ibomb.htm

Haeni, Reto, An introduction to information warfare, Washington DC: School of Engineering and Applied Sciences, George Washington University, December 1995.

http://www.seas.gwu.edu/student/reto/infowar/info-war.html

Institute for National Strategic Studies (INSS), *Strategic Assessment 1996: Instruments of U. S. Power*, Washington DC: National Defense University, 1996.

http://www.ndu.edu/ndu/inss/sa96/sa96cont.html

James, Shawn D. (Lt, USN), Information Warfare: A Phenomenon, an Innovation, or a New Paradigm?, Monterey CA: Naval Postgraduate School, 24 March 1995.

http://vislab-www.nps.navy.mil/~sdjames/IWpaper.html

Johnson, Stuart E., and Martin C. Libicki (eds.), *Dominant Battlespace Knowledge: The Winning Edge.*

http://www.ndu.edu:80/ndu/inss/books/dbk/

Libicki, M. C., What is information warfare? National Defense University Strategic Forum Report Number 28, May 1995.

http:/ /198.80.36.91/ndu/inss/strforum/forum28.html.

Libicki, Martin C. The Mesh and the Net: Speculations on Armed Conflict in a Time of Free Silicon. Washington, D.C.: National Defense University, McNair Paper no. 28, March 1994.

http://198.80.36.91/ndu/inss/macnair/mcnair28/m028cont.html

Magsig, Daniel E., Information Warfare in the Information Age, Washington DC: George Washington University, December 7, 1995.

http://www.seas.gwu.edu/student/dmagsig/infowar.html

MITRE Corporation, *The Information Warfare Awareness Primer*, downloadable presentation file for PC / Windows users.

http://www.mitre.org/capabil/training/TSG/Proj/IW/IWhome.html

Munro, Neil, The Pentagon's New Nightmare: An Electronic Pearl Harbor, *Washington Post*, Sunday, July 16, 1995.

http://vislab-www.nps.navy.mil/~sdjames/pentagon_nightmare.html

RAND Corporation. *Rand Research Review*, Vol. 19:2 (Fall 1995) Special Issue on Information War and Cyberspace Security.

http://www.rand.org/publications/RRR/RRR.fall95.cyber/index.html

RAND Corporation (1995d). The fly on the wall and the Jedi Knight, Research Brief (abstract) for Hundley, Richard O,. and Eugene C. Gritton, *Future Technology-Driven Revolutions in Military Operations: Results of a Workshop*, RAND Report DB-110-ARPA, 1995.

http://www.rand.org:/publications/RB/RB7104/RB7104.html

Sun Tzu on the Art of War, Gutenberg Project electronic text (public domain transcription of Giles, 1910), 1994. NOTE: The later Griffith translation is considered the canonical one.

http://all.net/books/tzu/tzu.html

Swett, Charles, Strategic Assessment: The Internet, Asst. for Strategic Assessment Office of the Asst. Secretary of Defense for Special Operations and Low-Intensity Conflict (Policy Planning), 1995.

http://www.fas.org/pub/gen/fas/cp/swett.html

Toffler, Alvin, The *Wired* interview, *Wired*, vol. 1.5 (November 1993), pp. 61 ff. Text available through *HotWired* WWW site at:

http://www.hotwired.com/wired/1.5/features/toffler.html